GC33-6077-1
File No. S370/4300-20

Program Product

Data Security Under the VSE System

Program Number 5746-XE9

Release 2

IBM

GC33-6077-1
File No. S370/4300-20

Program Product

Data Security Under the VSE System

Program Number 5746-XE9

Release 2

IBM

Summary of Amendments

This edition documents the following new or additional data protection features:

- Protection of private libraries in a chained library environmenl
- DL/I field level sensitivity

In addition, technical and editiorial changes were made throughout the book.

Significant changes are indicated by a vertial line to the left of the change.

Second Edition (October 1979)

This is a major revision of, and obsoletes, GC33-6077-0.

This edition applies to Release 2 of VSE/Advanced Functions and to all subsequent releases until otherwise indicated in new editions or Technical Newsletters. Changes are continually made to the information herein; before using this publication in connection with the operation of IBM systems, consult the latest *IBM System/370 Bibliography,* GC20-0001, for the editions that are applicable and current.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming, or services in your country.

Publications are not stocked at the address given below; requests for copies of IBM publications should be made to your IBM representative or to the IBM branch office serving your locality.

A form for readers' comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM Laboratory, Programming Publications Department, Schoenaicher Strasse 220, D-7030 Boeblingen, Germany. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation whatever. You may, of course, continue to use the information you supply.

Preface

This manual provides information for the user of the VSE system, who is concerned with data security and wants to become familiar with the available data protection facilities. The reader should be familiar with the functions and services as described in the *Introduction to the VSE System* and in the *VSE/Advanced Functions System Management Guide.*

This manual does not attempt to cover all aspects of data security and the implications involved. It introduces general aspects of data security, and concentrates on access control functions and system facilities that help to prevent inadvertent or intentional misuse of data.

The publication does not cover the subject of data backup and recovery. This topic is discussed in detail in the appropriate program product publications.

The manual is divided into chapters as follows:

Chapter 1: General Aspects of Data Security.

This chapter introduces general aspects of data security to make management and users aware of the problem areas of data security, with special regard to recent trends in the area of data processing. Hardware and software aspects are introduced.

Chapter 2: Security Features of IBM Hardware.

This chapter describes hardware security features (some of which are software supported) utilized by VSE/Advanced Functions the minimum IBM-supplied operating system support for the VSE system.

Chapter 3: Data Protection Facilities Available with the VSE System.

This chapter discusses standard facilities for access control and for the protection of data during processing in a multiprogramming environment. The system requirements and capabilities of the access control function for interactive and batch applications are discussed. There is a description of how to install the access control function, and how the VSE/Access Control-Logging and Reporting program provides for auditing access to system resources. Finally, the chapter addresses the subject of integrity, underlining the management and user responsibility in this regard and recommends a set of rules to enhance integrity.

Chapter 4: Protection Facilities Available with Optional Program Products.

This chapter gives an overview of the protection capabilities of a number of widely used optional program products.

Related publications are listed at the end of chapters 1, 3, and 4.

Contents

List of Figures

Chapter 1: General Aspects of Data Security

The Need for Data Security

Data security involves the protection of information from unauthorized or accidental modification, destruction and disclosure.

Most data processing installations are interested in data security for two basic reasons:

- To better protect the **assets** of the enterprise that reside within the computer system.
- To align business practice with the need for increased attention to the **privacy** of information about people.

Most organizations that use computers experience a growing level of dependence on the continued availability of the EDP system, its programs, and online data. Information processed by computer represents a major enterprise asset. It was acquired at significant cost; it constitutes an essential requirement to the continued functioning of the organization; and some portion of it is probably private or confidential.

Managers of computer facilities today are usually well aware of the need for safeguarding and protecting system resources from a variety of possible threats, and for complying with the ethical and legal principle of privacy protection. They see the needs for programmed aids in this area.

The Data Processing Environment

The advances made in data processing technology, hardware as well as software, make new and much more complex applications possible. The most important changes have been

- the increase in internal processing speed of the computer,
- the availability of more storage at a lower price,
- the development and implementation of DB/DC and interactive systems, resulting from the above changes.

More and more data processing installations make use of DB/DC and interactive facilities. This results in highly complex data processing environments, where many different applications and jobs can be run concurrently, and where, at the same time, a large number of terminal users may have direct access to the computer.

For such environments data security is obviously of greater importance than for a system that is used only for batch processing.

Direct and remote access to data via terminals poses a particular threat to the security of a system. Once the dialogue between the computer and the remote terminal has been established, virtually all the data, including the programs of the system, are potentially available to the terminal user, unless there is some sort of protection mechanism.

In a batch environment we have a human intermediary (job preparation, operator) between the user and the computer which reduces some risks, but at the same time may introduce others. Here too, control measures are necessary.

Figure 1 shows the relationship between system complexity and risk increase.

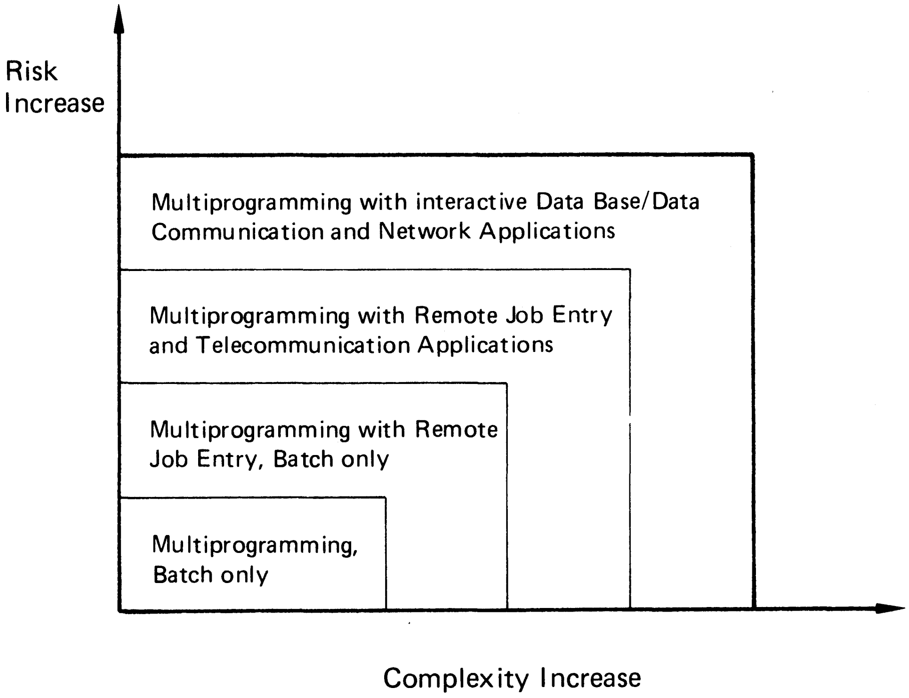

Risk Increase
Multiprogramming with interactive Data Base/Data Communication and Network Applications
Multiprogramming with Remote Job Entry and Telecommunication Applications
Multiprogramming with Remote Job Entry, Batch only
Multiprogramming, Batch only
Complexity Increase

Figure 1. System Complexity and Risk Increase Relation

To establish meaningful data security procedures for a given installation, the following three steps should be considered:

- Determining the **threats and hazards** to which a computer facility is subject.
- Deciding which system resources warrant special protection, estimating their value, and determining the specific risks to which they are exposed. This process is usually called **risk assessment.**
- Finally, deciding which **protective measures** are most appropriate, based on the results of the first two steps.

These three areas are briefly described below.

Threats and Hazards

There is substantial opinion and evidence that the most frequently occurring hazards that may cause destruction or unauthorized modification and disclosure of data are these:

- Errors and omissions:
  Most, installation managers agree that this is the most frequently occurring type of problem. Its source is well meaning, honest employees whose mistakes can cause losses running the full range from trivial to severe, from momentary to perpetual, from negligible to devastating.
- Dishonest employees:
  Computer related theft rates high; this hazard definitely deserves attention because systems are certainly vulnerable to the 'insider' intent upon fraud.
- Fire:
  This is important because it poses a threat both to the lives and safety of staff and to the basic mission capability of the installation. Although computer devices and components themselves are not highly flammable, the paper products likely to be found in the vicinity are a potential source of combustion, and computers are subject to severe damage from heat and soot.
- Water:
  Damage from water may be the result of extinguishing fire or of flooding, either from natural causes or from plumbing accidents.
- Disgruntled employees:
  Such individuals are motivated by a wish to inflict damage rather than by financial gain. Also, unlike dishonest employees, disgruntled employees are frequently indifferent to or may even seek, exposure. Enlightened personnel practices and sensitive, astute, aware management are the best preventatives against threats from dishonest or disgruntled employees.

There are, of course, threats, such as those posed by riot and war, by industrial espionage through wire tapping or theft from an outside source or by the interception of electro-magnetic emanations. Although they have a dramatic nature and, when exposed, are widely reported, their frequency is probably substantially less than the threats discussed above.

Each type of threat need not necessarily have its own unique series of protective measures. Certain measures may help thwart more than one threat. The computer, of course, knows nothing of motives; it cannot distinguish between errors and deliberate violations of security. So the user who has taken steps to minimize the chances of error has gone a long way in protecting against the intentional misuse of his system's data.

Risk Assessment

In order to be sure that the security measures to be chosen are the most cost-effective ones, a risk assessment should be done. There are different techniques for doing this, but they essentially involve calculating (1) the likelihood of something to happen, and (2) the approximate cost resulting from such an event, and then using some portion of that calculated cost to finance appropriate counter measures.

For more details, see *A Guide to Risk Assessment and Choice of Measures.*

Protective Measures

There is no single formula for data security, no single product or technique that provides complete protection. An effective data security program is made up of a combination of measures. Figure 2 depicts the nucleus of data surrounded by several concentric rings of protective measures. Each ring is a broad category to be filled with specific measures tailored to the needs and environment of each particular installation. Some examples of the kinds of questions to be asked and techniques to be evaluated in each of the three areas are these:

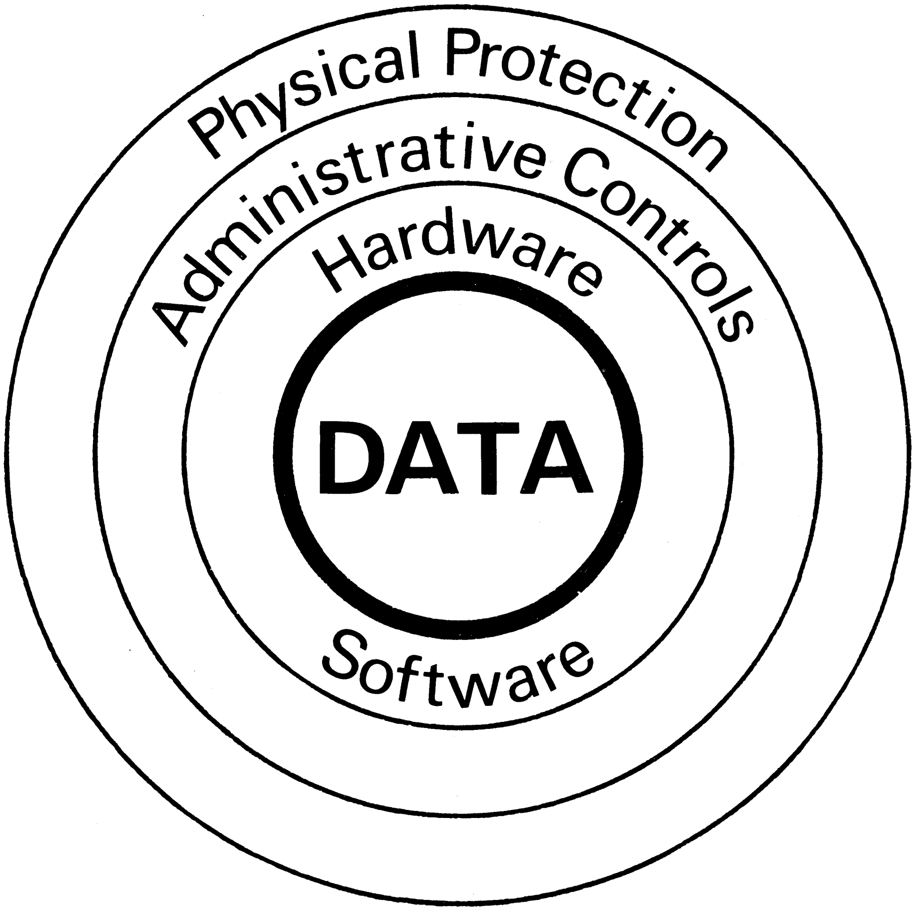
Physical Protection

Consider the structure that houses the computer. What kind of building is it: Old or new construction, high-rise urban site, or low profile country 'island' facility? Who else occupies the building? Which floor is it on? Who has access to that floor? What kind of people are employed in the computer room?

There may be fences to enclose the building and guards at the gate or at the door to make sure that only authorized people can enter. Basic are fire and smoke detection and fire extinguishing devices. In most computer facilities, blast resistant walls have replaced the large plate glass windows, popular some years ago. Access to the machine room itself must be rigidly controlled and even such considerations as the location of the car parking area and the machine room's proximity to the 'utility core' of a modern office building play a role in a total security plan.

Emergencies must be anticipated. Every computer operation should have a 'disaster plan' for hardware and site back-up, for alternate power and communication facilities, as well as for program and data reconstruction.

Several of the publications listed at the end of this chapter provide guidance on the various aspects of physical security.



A comprehensive data security program must consider measures in each of these areas.

Figure 2. Areas of Data Security

Administrative Controls

This is a very broad category, with data security implications in many diverse areas. Again, only a few examples are mentioned here. Additional references listed at the end of the chapter can provide greater depth.

Personnel practices of an organization affect security. For example, how do you screen and hire application and system programmers, operators and analysts? Is there some system of periodic job rotation? Are annual vacations required to be taken?

Has every step of machine room operations been scrutinized for security implications? For example, how are discarded listings, carbon paper and printer ribbons disposed of? How is input work to the computer screened to make sure that it does not do any harm to the data that is kept online; how is batch output from the computer room distributed — the printed data, the program listings, and the memory dumps that go back to users and to application developers?

Program development and maintenance is another important area where a range of security measures must be present and enforced. Organizational procedures, once established, must be observed. Are incompatible jobs done by the same person? For example, is the person who is authorized to add new suppliers to the master vendor file the same individual who authorizes invoices for payment? If so, there is a data security exposure.

There is no substitute for an effective audit. Manual control and review are still required. The human element must be present. Variance checking and follow-up are absolute requirements for an effective administrative program. All of these functions are the traditional realm of the auditor, and they should not be neglected.

Hardware and Software Measures

Finally, there are hardware and software measures that help protect data. These may be simple, familiar things, like a key-lock or badge reader on a terminal, the write-protect ring on a reel of tape, the write-inhibit switch in a disk drive, or the storage protect capability of processors. Other measures, such as cryptography, are highly specialized techniques, intended to protect data under very specific circumstances.

When a user sits in front of a terminal connected to the computer, the most practical way of ensuring that he conforms to the security rules is by means of a software mechanism controlling that user's access to the system, to programs, and to data. Most access control procedures have certain elements in common. These elements are introduced below.

Identification and Authentication

Before the user is allowed access to system resources he must identify himself and that identity must be verified. For a terminal user this verification is done during the log-on procedure; for a batch user it may be accomplished by means of job control statements.

For both steps the user must provide information that agrees with the information stored in the system. In the first step the user identifies himself. If the system finds identical user data it initiates the second step by requesting the user to provide his password for authentication, that is the verification of his identity. Only if the password provided is the same as the one stored in the system, is the user allowed access to the system.

Passwords should be changed from time to time to reduce the possibility of a password becoming known to unauthorized persons.

Authorization

Authorization deals with the protection of resources: files, libraries, and programs, for example. Good security practice requires that a user should be restricted to those resources he needs to do his job.

Each resource to be protected must be defined to the system and each such resource definition must contain information that precisely defines the security status of the resource. The system compares this information with the information provided by the user and only in case of a match is the user allowed access to this specific resource.

Logging

To be able to audit a system and identify attempted or committed security violations, security related events must be logged automatically. An event may be defined as any access to a protected resource or any attempt to access the resource without authorization. The logging record should contain only information needed for the identification of the particular resource and of the user accessing or attempting to access the resource. By no means should this record include any security sensitive information. A program is required to edit and to print the logged event records and to produce suitable audit reports.

Auditing

Careful analysis of audit reports may well result in the discovery of security violations and may also disclose the identity of the user(s) associated with them. Moreover, audit reports can provide important indications for management regarding the overall security status of the system.

General Data Security Considerations

It is obvious, when considering the full scope of data security, that many measures are in areas where IBM cannot provide direct assistance in the form of products. Hardware and software components certainly form a part of a total security program, and the facilities described in the following chapters can be significant contributions to a total security plan. But they are not a substitute for the physical measures and administrative controls that must also be present; and they are not a substitute for the most essential ingredient of a total security plan: management interest and involvement and management participation and control, all on a continuing basis.

A VSE system has a number of security features and protection facilities available, and these are found in different components of the hardware and software; they are discussed in the subsequent chapters:

- Security Features of IBM Hardware (Chapter 2).
- Data Protection Facilities Available with the VSE System (Chapter 3).
- Protection Facilities Available with Optional Program Products (Chapter 4).

Related Publications

Following are some of the IBM publications pertaining to the broad aspects of computer security:

The Considerations of Physical Security in a Computer Environment, G520-2700
The Considerations of Data Security in a Computer Environment, G520-2169.
Data Security Controls and Procedures -
A Philosophy for DP Installations, G320-5649
42 Suggestions for Improving Security in Data Processing Operations, G520-2797
Management Controls for Data Processing, GF20-0006
Management Memorandum: Security Features of System/370, G320-5650

Data Security through Cryptography, GC22-9062
IBM 3845/3846 Data Encryption Devices, General Information, GA27-2865

Systems Auditability & Control/Audit Practices, G320-5790
Systems Auditability & Control/Executive Report, G320-5791
Systems Auditability & Control/Control Practices, G320-5792

The following manuals make up the *Data Security Design Handbook.* The complete set may be ordered by using order number GBOF-7502.

Data Security - A Summary for Executives, GE19-5232
Data Security - Planning and Control, GE19-5231
A Guide to the Analysis of Deficiencies in and Threats to Computer Operations, GE19-5211

A Guide to Risk Assessment and Choice of Measures, GE19-5230
A Guide to the Design of Data Protection Measures, GE19-5233
A Guide to Education in Data Security, GE19-5229

Data Security Study Site Publications:

Volume 1, Introduction and Overview, G320-1370
Volume 2, Study Summary, G320-1371

Chapter 2: Security Features of IBM Hardware

A variety of security features is available in the hardware area, and some of them are realized through software support.

The available security features provide for integrity of the system to some extent, that is, they serve as safeguards against unintentional destruction of data during processing.

Other security features have been designed for controlling the physical access to a device, or for preventing the unauthorized removal of a disk pack, for example.

This chapter discusses the standard security features available with IBM hardware.

Central Processors

The integrity of central processing units is ensured by a number of familiar features such as parity checking.

The storage protection key, normally set under the control of the operating system, provides protection against inadvertent data overwrite in processor storage, particularly in a multiprogramming environment.

Magnetic Tape Units

To discuss the security features available with magnetic tape units, the IBM 3420 Magnetic Tape Unit is used as an example. The following features are available:

File protect ring
Parity checking
Data security erase

- The file protect ring is used to prevent unintentional writing on the tape. Writing is permitted only if the file protect ring is mounted.
- Parity checking is done during tape read and write operations.
- The data security erase feature is software supported and allows the erasure of sensitive data from the tape.

Direct Access Storage Devices

To demonstrate the security features of direct access storage devices, the IBM 3330 Disk Storage is used as an example. The following features are available:

Write inhibit switch

Positive seek verification
Drawer open keylock (optional)
Pack to spindle (optional)

- The write inhibit switch can be used to prevent unintentional or unauthorized writing on the mounted disk pack, if all of the data stored on the pack is of the read-only type.
- The positive seek verification ensures that the read/write head has been positioned over the track that is to be accessed.
- The drawer open keylock allows the locking of the drawer to control the physical access to the disk pack.
- A mechanism allows the locking of the disk pack to the spindle to prevent a removal of the pack.

Other DASD devices such as 3340, 3344 and 3350 offer positive seek verification, as well as a read only or write inhibit switch, as described for the 3330 DASD device.

DASD file protection is available as software support and is specified at system generation time. This facility is described in Chapter 3.

Diskettes

Data protection for diskette volumes is available as software support and is discussed in Chapter 3.

Data Communication Terminals

Various terminals offer one or more of the following security features:

Display suppress
Print inhibit
Keylock
Magnetic stripe card reader

- The display suppress function, if used, prevents data that is being entered to be also displayed on the screen. The function is useful, for example, when sensitive data (such as a password) is being entered.
- The print inhibit function allows to suppress the printing of sensitive data on an associated printer when being entered.
- The keylock and the magnetic stripe card reader serve to allow only authorized users access to the terminal.

For terminals that do not offer the display suppress function, programming techniques, such as repetitive typing or backspacing of multiple characters, may be used in the display area to obscure sensitive data.

Data Encryption Devices

The transmission of sensitive data over communication lines, outside the protected and controlled computer room environment, causes a security risk. This exposure can be overcome by the installation of data encryption devices. One such device is installed at each end of a communication line and all data that passes between the two locations is enciphered, making it unintelligible to anyone not having the 'secret' key.

The IBM 3845 and IBM 3846 data encryption devices serve this purpose.

Chapter 3: Data Protection Facilities Available with the VSE System

This chapter describes standard facilities for protecting data. It introduces the access control function of the VSE system which offers an acceptable level of protection against unauthorized access to the system and its resources. It describes the capabilities and the components of the access control function and how to install it. The chapter concludes with a discussion of the subject of integrity and the role of the security administrator.

Standard Facilities

IPL User Exit

It may be desirable to perform certain integrity and security checks at the end of an IPL procedure: whether the right system pack was mounted, or whether the correct data was entered for the new work session; for example, if working with labeled files, it is important that they bear the correct creation date, so as to provide for their protection until their expiration date.

An exit routine might also issue a request for the operator to enter an installation defined security code with two retries (in case of a typing error). The routine could, if a wrong security code was submitted three times, go into a continuous loop that displays (or prints) on the console one blank line after another. To get out of this loop, the operator would have to reset the CPU and start the IPL procedure from the beginning.

After the IPL procedure has been completed, control is passed to the phase $SYSOPEN. This phase, a dummy phase in the IBM supplied system core image library, can be replaced by a user exit routine to perform various checks that may be important for the security and integrity of the system. For more information on the IPL user exit refer to the *VSE/Advanced Functions System Management Guide.*

Job Control User Exit

This standard facility can be used for access control; but it requires a great deal of programming effort for implementation and again for extension, should this become necessary. Using the new access control function (discussed later in this chapter) definitely is the better approach. The facility transfers control to a routine in the shared virtual area (SVA) each time a job control statement has been read. The routine is loaded into the SVA at IPL time; it is cataloged in the core image library under the name of $JOBEXIT. This phase, a dummy phase in the IBM supplied system core image library, can be replaced by a user exit routine to perform various access control checks.

While a user-written job control exit routine may be used to dynamically change the operands, it is certainly useful to check whether installation defined program usage authorization exists. For example, to check the usage authorization for a program named PRIVLGE, the exit routine could be designed to examine the // EXEC statement for a specific code in the comment field as shown below:

user specification:	// EXEC PRIVLGE	(no code specified as a comment)
replacement by the user exit routine:	// EXEC ERROR1	

where program ERROR1 might simply issue a message indicating that the job cannot be processed due to a missing usage code.

The routine might also be used to examine an installation defined data access job identification code in the // JOB statement, and compare this code with an access authority code which the owner of the file to be accessed had defined when the particular file was created. The user exit routine is not allowed to perform any I/O operations, to issue any SVC's, or to cancel the job.

For more information on the job control user exit refer to the *VSE/Advanced Functions System Management Guide.*

Labeling

Labeling helps to ensure that the correct data is mounted for processing and assists in protecting data against

- inadvertent destruction, and
- unauthorized access and usage.

This protection is provided for files stored on magnetic tape, disk, or diskette, where each file is identified by one or more file labels. In addition, each volume of data is identified by one volume label.

Volume and file labels are mandatory for disks and diskettes, and optional for tapes. For security reasons, however, it is strongly recommended to work with labeled tapes only.

The TLBL statement is used for specifying label information for a magnetic tape, the DLBL and EXTENT statements for specifying it for a DASD device, or a diskette. The system provided label processing routines check whether the correct volume is mounted, whether the retention period or expiration date is still valid, so as to protect output files from being overwritten and destroyed prematurely.

At file creaticn time the contents of the label has to be specified. The same label information must be available at processing time to enable the system to compare the actual label of the data being processed with the label information submitted by the user. If a mismatch is detected the job is terminated.

For more information on labeling refer to the *VSE/Advanced Functions System Management Guide.*

Data Secured Files

The DSF parameter in the DLBL statement indicates that a data secured file is to be created or processed. If a data secured file is to be accessed, a warning message is issued on the console. The operator then has to decide whether this file can be accessed by the program causing the message. All these warning messages would make up a record of file accesses. While this method may have provided sufficient protection of and privacy for an installation's data in the past, it may not meet the protection and privacy standards of the future. Using the access control function of the VSE system (discussed later in this chapter) is the method to be preferred.

Diskette File Protection

The following protection features are available for data on a diskette:

- The volume accessibility indicator in the volume label is checked by the operating system for input and output. If the volume is marked as secured (inaccessible), a message is issued on the console, and the operator must decide whether the program causing the message is allowed to access the volume.
- The file security indicator in each HDR1 label is checked for all input files. By using IOCS, the user can create a secured file at output time. If, when used as input, the file is recognized as secured, a message is issued on the console, and the operator must decide whether or not the program causing the message is allowed to access the file.

  If a secured file is being created, the volume label is also updated to indicate the volume as secured (inaccessible).
- If the file is marked as write-protected in the HDR1 label, the file cannot be overwritten by IOCS.
- By specifying an expiration date, a file can be protected against being overwritten within the specified period of time.

DASD File Protection

This facility prevents programs from writing data outside the limits of their disk files. This might happen if, for example, a randomizing algorithm produces an unexpected DASD address which is outside the file limits. Other files on a DASD device are thus protected against unintended destruction. However, if two DASD files have been opened in the same partition and use the same programmer logical unit, these two files are not protected against destroying each others data.

DASD file protection is supported if the DASDFP parameter is specified in the FOPT supervisor generation macro.

For more information on DASD file protection refer to the *VSE/Advanced Functions System Management Guide.*

Track Hold Option

In a multiprogramming environment this facility prevents two or more programs from concurrently updating the same record of a track on a CKD-type DASD, or the same record within the range of a block on a FBA-type DASD. In an installation that makes effective use of this facility, all of an installation's programs should specify track hold in their DTF's. Track hold support is available if the TRKHLD parameter in the FOPT supervisor generation macro was specified for supervisor assembly. For more information on the track hold option refer to the *VSE/Advanced Functions System Management Guide.*

Resource Protection Through Macros

In a multitasking environment a mechanism is needed to prevent a task from using the resources of another task in an uncontrolled way, so as to avoid the destruction and erroneous updating of data. The lock management protects user-defined and system resources against concurrent use by different tasks in different partitions.

Two levels of sharing are available when using the IBM-supplied LOCK and UNLOCK macros:

- Exclusive usage of a resource.
- Shared usage of a resource.

The following resources may be protected:

Files, libraries, catalogs, disk volumes and control blocks.

The resources are defined by symbolic names. Any symbolic name may be used; however, a naming convention should be established for the installation, and should be adhered to by all programmers using the LOCK and UNLOCK macros. A file name, a volume-id (VOLID), or a DASD file begin address are examples of symbolic names.

The DTL and GENDTL macros are available to define a resource for share control. The DTL macros builds a lock control block, which the operating system needs to control the sharing of the particular resource during assembly; the GENDTL macro builds this block dynamically during execution.

Once the lock control block is defined for a resource, the operating system can efficiently control exclusive or shared access to the resource in accordance with the DTL or GENDTL macro. The MODDTL macro allows a lock control block to be modified dynamically.

A successful lock request (via the LOCK macro) means that the resource is locked for the task or partition issuing the request. With the UNLOCK macro the program can either release the resource completely, or in conjunction with the MODDTL macro, weaken the lock control from 'exclusive control' to a shared status.

For more information on the various macros refer to the *VSE/Advanced Functions Macro User's Guide,* and the *VSE/Advanced Functions Macro Reference* manual.

Reliability Data

The reliability data extractor (RDE) is a standard support which records the reason for every IPL performed. At the time the first // JOB statement after IPL is processed, a message on SYSLOG requests the operator to submit a two-character IPL reason code. On the basis of these replies job control builds a record for SYSREC. A listing of this file can be obtained by running the EREP program. By regularly reviewing EREP listings of recorded IPL events, management may well be capable of detecting unauthorized usage of the computing system (IPL between the last shift of one day and the first shift of the next, for example).

For more information on reliability data refer to *VSE/Advanced Functions System Management Guide.*

Access Control Function of the VSE System

The access control function of the VSE system is a tool that helps the user to implement an acceptable degree of data security. It assists a user in addressing requirements made by national data security laws (such as personal accountability) and provides support for:

Identification and Authentication

Authorization

Logging and Reporting

Auditing

The above software measures are briefly discussed under *Hardware and Software Measures* in Chapter 1.

The access control function, which is available at installations whose VSE system includes the VSE/Interactive Computing and Control Facility (VSE/ICCF), offers access control for batch and/or interactive applications. Its significant advantages are:

- It frees the user from devising and writing his own access control software.
- It offers access control functions that can easily be adjusted to a changing and expanding environment.

System Requirements for Implementation

To make use of all the facilities offered by the access control function the following options and components must be supported or must be part of the system:

- The system's supervisor has to be generated with SEC=n in the FOPT generation macro.
- The VSE/Interactive Computing and Control Facility (VSE/ICCF). This licensed program requires a partition of its own, or may co-reside in a partition with CICS/VS if this terminal control system is used.

  To IPL successfully a supervisor generated with SEC=n VSE/ICCF must be installed.

The VSE/Access Control-Logging and Reporting program, although not a requirement, is needed if an installation plans to keep track of the usage of certain protected programs and data. The program supports the logging of attempts to use protected resources without authorization and, optionally, of any access to or use of protected data and programs. It provides formatted reports of the information logged. This licensed program requires the 'Compare and Swap' hardware feature.

The access control function can be used without the logging and reporting program being installed.

Concepts

Figure 3 gives an overview of the access control function of the VSE system. This overview shows that the control function does security checking on two distinct levels:

- User identification and authentication — is the user permitted to use the system at all.
- Resource and data use/access authority — is the user permitted to invoke a particular program, or to access a particular file or library.

Each of these types of checking is discussed in more detail later in this section. To do this checking the access control function needs a user provided access control table, which is briefly discussed below.

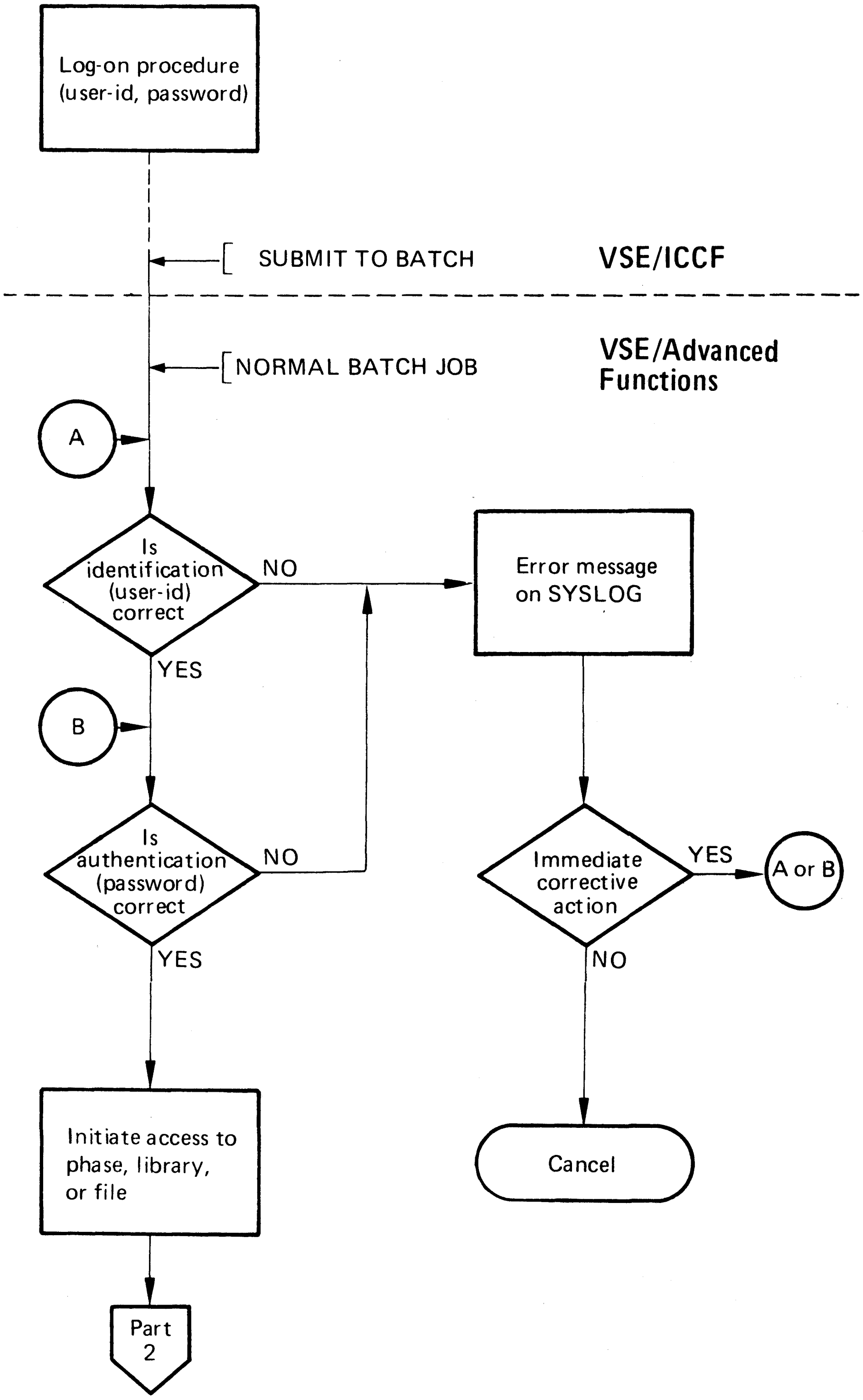

Log-on procedure (user-id, password)
SUBMIT TO BATCH
VSE/ICCF
NORMAL BATCH JOB
VSE/Advanced Functions
A
Is identification (user-id) correct
NO
YES
Error message on SYSLOG
B
Is authentication (password) correct
NO
YES
Immediate corrective action
YES
A or B
NO
Initiate access to phase, library, or file
Cancel
Part 2

Figure 3. Overall Structure of the Access Control Function of the VSE System (Part 1 of 2)

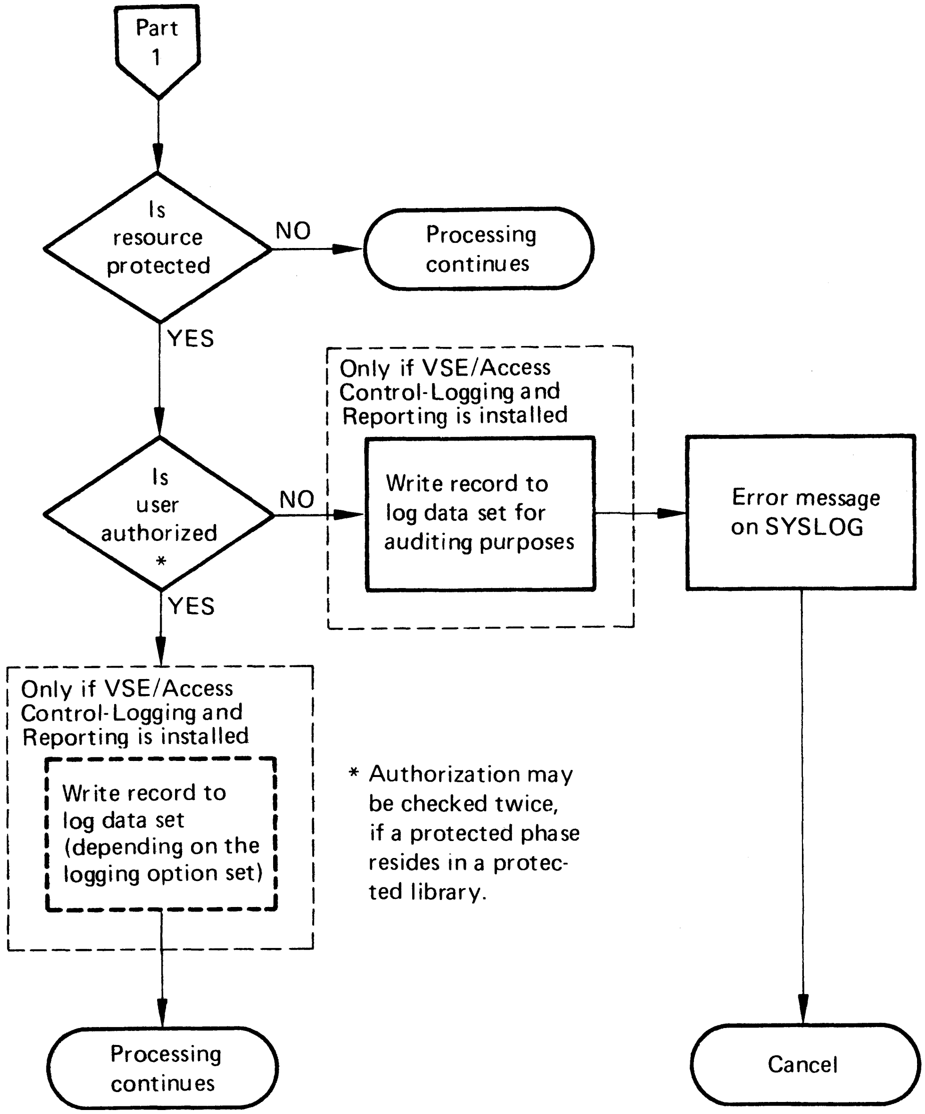

Part 1
Is resource protected
NO
Processing continues
YES
Only if VSE/Access Control-Logging and Reporting is installed
Is user authorized *
NO
Write record to log data set for auditing purposes
Error message on SYSLOG
YES
Only if VSE/Access Control-Logging and Reporting is installed
Write record to log data set (depending on the logging option set)
* Authorization may be checked twice, if a protected phase resides in a protected library.
Processing continues
Cancel

Figure 3. Overall Structure of the Access Control Function of the VSE System (Part 2 of 2)

The Access Control Table (DTSECTAB)

The access control table contains all the information necessary for the system to perform access authorization checking. This information is stored in two types of entries: user profile and resource profile entries.

The information stored in a user profile entry includes the user identifier and his password for identification and authentication checking, and the access control class(es), possibly an update indication for authorization checking.

The information stored in a resource profile entry includes the resource name, the access control class(es) for authorization checking, and the logging option(s) for either recording all accesses to this resource, or only the violations.

Normally, it is the security administrator who personally defines and updates the access control table of his system. The table gives the security administrator a centralized view of access control within the entire system. How the table is defined and updated is discussed under *Implementation* later in this chapter.

Figure 4. shows how the access control table is used by the access control function.

Note: VSE/ICCF uses its own table, called user profile (located in the VSE/ICCF library), for the identification and authentication check during the VSE/ICCF log-on procedure. A VSE/ICCF user submitting jobs for processing in a batch partition of the system must also be defined in the access control table (DTSECTAB).

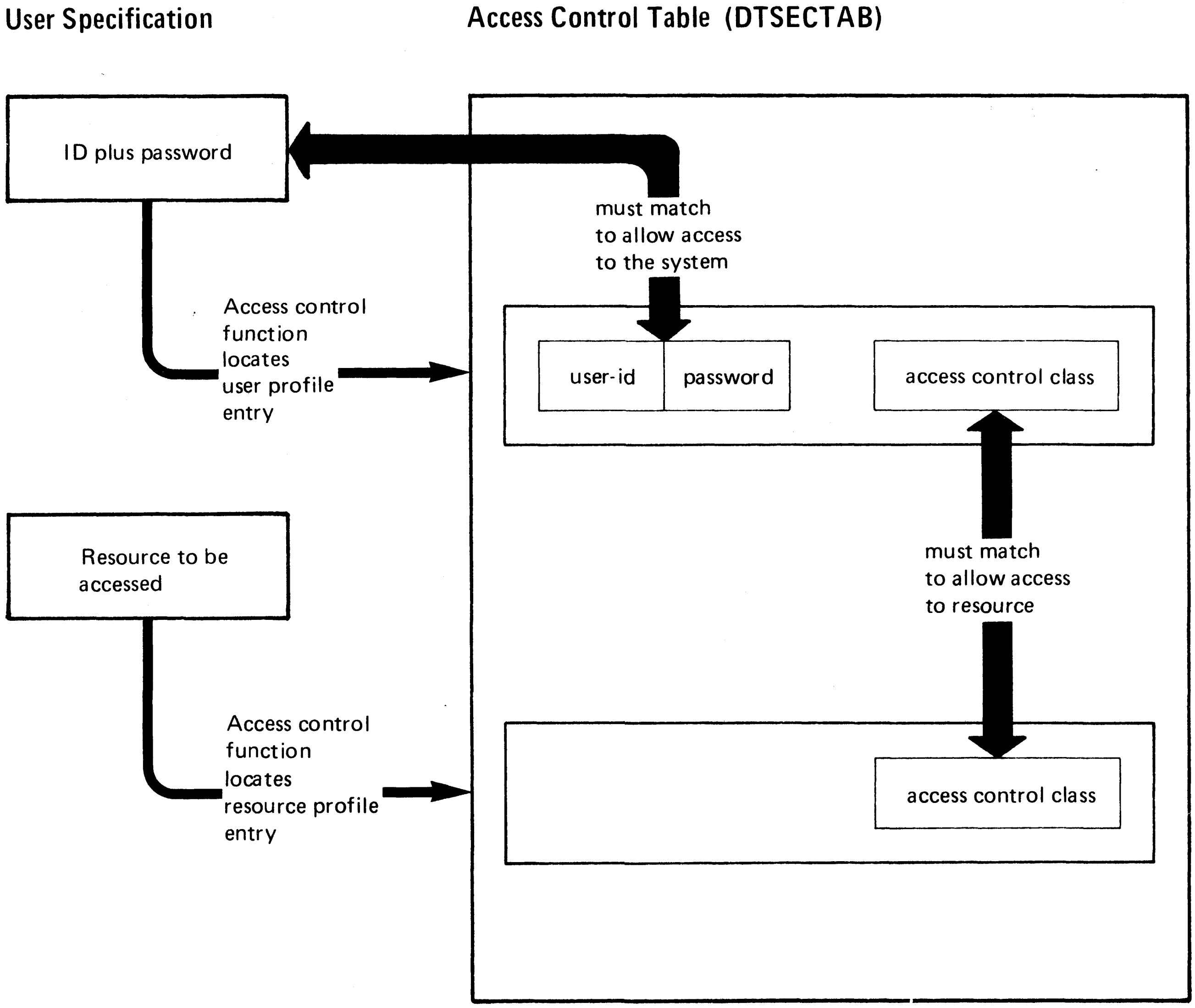


Figure 4. Concept of Access Control

User Identification and Authentication

Interactive Processing

For an interactive terminal user, the identification and authentication check is usually done during the log-on procedure. This is also true for a VSE/ICCF user. Having encountered a request for log-on with user-ID, VSE/ICCF searches for the corresponding user profile record. If it is found, the system prompts the user to supply his password for authentication and compares it with the one stored in that user's profile record. Only if both terms agree is the user logged on to the system. He may now work with VSE/ICCF, that is, have programs executed in interactive partitions or work with the VSE/ICCF editor, or submit jobs for processing in a batch partition of the system, or both.

The access control aspects for an VSE/ICCF user who also submits jobs for processing in a batch partition of the system, and for a user submitting jobs for batch processing through VSE/POWER or directly are described below. For the access control aspects of a VSE/ICCF only user, working with interactive partitions only, refer to Chapter 4, where the access control facilities of VSE/ICCF are discussed.

Batch Processing

To allow the identification and authentication of a batch user, a job control statement has been introduced; the // ID statement. It should be placed behind the // JOB statement and must contain the user identification and password. The format is as follows:

// ID USER=user-id,PWD=password

USER=Specifies the user identifier and must be 4 alphameric characters long.

PWD= Specifies the user password and can be 3 to 6 alphameric characters long.

It is possible to run jobs without an ID statement (for compatibility reasons), but the job is canceled as soon as an access to a protected resource is attempted. However, if the access control function is installed, it is advisable to introduce the ID statement for the whole system to force a user to identify himself, and to avoid possible security exposures.

Two types of batch applications with regard to identification and verification can be distinguished:

1. *'Pure' batch:* Submission of the job stream from a card reader (which may or may not be spooled by VSE/POWER).

   The system reads the specified user-ID and searches for the corresponding user profile entry in the access control table; if that entry is found, the system compares the password with the one supplied in the ID statement. If they are identical, processing continues. If the specified user-ID or password is not known to the system an error message is issued on SYSLOG, and the job is canceled if the input is from

SYSRDR, and a job statement is present, and the NOLOG option is in effect; otherwise the system waits for corrective action.

2. *Submitted batch:* Submission of the job stream from a VSE/ICCF controlled terminal for execution in a (non-interactive) partition of the system.

   Before a terminal user can submit a job for batch processing his identity and password were verified during the VSE/ICCF log-on procedure.

   The // ID statement for a job to be submitted is supplied in two ways:

   - If the job control statements for the job to be submitted are created by VSE/ICCF, VSE/ICCF also creates the // ID statement using the information supplied during the log-on procedure.
   - If the user submits a job stream or a VSE/ICCF member that contains JCL statements, then the user must supply also the correct // ID statement.

   Verification of the // ID statement is the same as described under 1, above.

Access Authorization Checking

Resources to be protected must be defined in the access control table (DTSECTAB). The following resources can be protected:

1. Files
   - All disk files and labeled tape files defined by a file description macro DTFxx, or by appropriate file definition statements of the installation's IBM compiler(s).
   - VSE/VSAM catalogs.
2. Private libraries defined for the duration of a job (temporary) by a job control LIBDEF statement.
3. Phases
   - Phases in the system core image library
   - Phases in a private core image library

Moreover, resources may be protected in groups; that is, if a user specifies a group name, all resources whose initial characters match that group name are protected.

A total of 32 access control classes are available to be assigned to a resource, and an access control class can be defined with or without a logging option. If the logging option is set, all accesses to this resource are logged; if the option is not set, only the violations are logged.

The information of a user profile entry in DTSECTAB is compared with the information stored for the resource to be accessed by this user in the corresponding resource profile entry in DTSECTAB. This check is done in two steps:

1. A check for a match of the access control class.

   If thère is a match between the access control class of the user profile entry and the profile entry of the resource to be accessed, processing is allowed to continue. Otherwise, a security violation is indicated. This check is done for all resources.

2. A check for a match of the read/update indication.

   The check for the read/update indication depends on the file utilization, that is, whether the file has been opened for read or update.
   If there is a match between the read/update indication of the user profile entry and the file utilization, processing is allowed to continue. Otherwise, a security violation is indicated.

Note: A read-only authorization provides for acceptable update (write) protection only if the particular resource is a VSE/VSAM file. Therefore, non-VSE/VSAM files and libraries should be defined with update authorization.

In case of a violation, a message is issued on SYSLOG, the job or user program is canceled, and the violation is recorded on the log data set if the VSE/Access Control-Logging and Reporting program is included in the system.

Logging and Reporting

The licensed VSE/Access Control-Logging and Reporting program enables the security administrator to audit the access to system resources. The program logs access control related events and allows to print them later for analysis.

Whenever a logging situation occurs the logging and reporting program writes a record on the log data set, a file on disk, to record the event. Any programmer logical unit may be assigned to the disk volume which accomodates the data set needed for logging.

For each resource defined in DTSECTAB, a logging option can be specified. Depending on the specification of that option, either all accesses to this resource are logged, or only attempted access violations. For further details refer to the section *Defining the Access Control Table* later in this chapter.

The reporting module of the logging and reporting program, to be run in batch mode in a partition of the system, creates printouts from the log data set according to the specifications of the user. For more details on this topic, refer to the section *Auditing Access to Controlled Resources* later in this chapter.

For a complete description of the VSE/Access Control-Logging and Reporting program, refer to the appropriate IBM publications as listed at the end of this chapter.

Implementation of the Access Control Function

A supervisor supports the access control function of the VSE system if it was generated with SEC=n in the FOPT generation macro, where n defines the number of entries to be stored in the logging queue and thus determines the number of logging requests that can be processed concurrently. If heavy logging activity is anticipated (many protected resources and all accesses are to be logged) a correspondingly higher value should be specified.

Once a supervisor with access control support has been assembled and cataloged, and VSE/ICCF has been installed (required for a successful IPL of the supervisor), the following access control tables are needed for security checking:

- One such table (DTSECTAB) for jobs submitted for batch processing.
- Up to three (DTSM2 — the program table; DTSM6 — the file table; DTSM7 — the load-protection table) for jobs that are to be processed in an interactive partition under VSE/ICCF.

Defining a DTSECTAB control table is discussed below. For a detailed discussion of defining the tables DTSM2, DTSM6, and DTSM7, refer to the appropriate VSE/ICCF publication; for the purpose of these tables see Chapter 4 of this manual.

Defining the Access Control Table (DTSECTAB)

If available, DTSECTAB is loaded into the SVA during IPL, but it may be generated later as well. It is possible to update and catalog DTSECTAB during processing and the system will always use the latest version. No re-IPL is necessary as long as the SVA has sufficient space available for the new copy of the table. After a successful link editing of the table, the processing of the next // ID statement makes the new version available.

The access control table contains entries as follows:

- User entries:
  They define which users are allowed to use or access which resources.
- Group entries:
  They define groups of recources by the first or the first two to seven characters of the resource names.
- Library entries:
  They define, for private libraries, what authority users must have in order to access these libraries.

- File entries:
  They define the authority users must have in order to access the particular files.
- Phase entries:
  They define the authority users must have to invoke (by // EXEC) or load (by FETCH or LOAD) the named phases.

For each entry a user wants to have included in the table he must define a macro call (macro DTSECTAB) in the source language job stream which defines the access control table; a job stream of the type that would normally be written, assembled and executed by an installation's security administrator personally. Macro DTSECTAB is described and its format is shown in the Appendix at the end of this publication.

The example assumes that the required device assignments for the assembly and linkage editor runs were defined as permanent immediately after IPL.

```
// JOB GENERATE DTSECTAB
// ID USER=user-id,PWD=password
// OPTION CATAL,NOLIST
// EXEC ASSEMBLY
```

User entries

```
┌─ column 10                            column 72─┐
↓                                                 ↓
DTSECTAB TYPE=USER,                               X
         NAME=PAUL,                               X
         ACC=(1-32,U),                            X
         PASSWRD=XB3L25,                          X
         AUTH=YES,                                X
         SUBTYPE=INITIAL
         ↑
         └── column 16
```

User PAUL is defined as the security administrator (AUTH), who is authorized to access and update any protected resource. Only one such entry can be defined and is accepted by the system. The access control classes and the update option are indicated for the sake of clarity only, since the security administrator indication bypasses all access authorization checks, however, all accesses performed by the security administrator are logged.
SUBTYPE=INITIAL must be specified for the first macro call.

Parameters PASSWRD, AUTH and the update option U in the parameter ACC can be specified for user entries only.

Note: A read-only authorization provides for acceptable update (write) protection only if the particular resource is a VSE/VSAM file. Therefore, non-VSE/VSAM files and libraries should be defined with update authorization in the user entries.

```
DTSECTAB TYPE=USER,                X
         NAME=ANNA,                X
         ACC=(1-4),                X
         PASSWRD=CCK81P
```

User ANNA can only access resources defined with access control classes 1-4 and has no update authority for files or libraries.

```
DTSECTAB TYPE=USER,                X
         NAME=HUGO,                X
         ACC=(16,25,U),            X
         PASSWRD=693DE4
```

User HUGO can access only resources defined with access control classes 16 or 25, and he has update access to files and libraries of class 25.

```
DTSECTAB TYPE=USER,                X
         NAME=OTTO,                X
         ACC=(1-8,25-32,U),        X
         PASSWRD=7BMC3U
```

User OTTO can access resources defined with access control classes 1-8 and 25-32. He has update access to files and libraries of classes 25-32, and read only access for classes 1-8.

Group Entries

```
DTSECTAB TYPE=GROUP,               X
         NAME=PAYROL,              X
         ACC=(1-8),                X
         LOG=(1-8)
```

This group entry defines that any resources whose first 6 characters are PAYROL (for example PAYROL0 through PAYROL9) may be accessed by any user that has an access authority of classes 1 through 8. All accesses to this group of resources will be logged.

Group entries are scanned after the individual library, file, or phase entries. By assigning naming conventions within the data processing installation for libraries, files, and phases, which can be identified within groups, a better structure for controlling the access control function is achieved, and the size of the table is reduced to minimize updating and improve performance. Moreover, the use of group entries allows a user to define and create additional resources and have them protected without the need of updating and reassembling the control table. Adding a new resource named PAYROL1 would, in the above example, result in accessibility restricted to classes 1 through 8 for the resource PAYROL1.

Individual entries should be used only for resources that either are separate entities in the system, or for resources which are to be excluded from access by all users as they are defined in a group entry, for example. For consistency reasons, the individual library, file, or phase entries should contain access control classes that are a subset of those specified for group entries.

If the resource being validated does not have an individual entry but is covered by a group entry, the logging options of that group entry are in effect for that particular resource.

Logging options can only be specified for group, library, file, and phase entries.

```
DTSECTAB TYPE=GROUP,                    X
         NAME=EMIL,                     X
         ACC=(1-8,25,32),               X
         LOG=(1-8,25)
```

Group entry EMIL permits users defined with access control classes 1-8, 25 and 32 to access files, libraries or phases that begin with the character string EMIL.
The LOG specification causes all accesses for classes 1-8 and 25 to be logged. For access control class 32, only the access violations will be logged. The LOG specification is only meaningful if it agrees with one or more of the access control class specifications.

```
DTSECTAB TYPE=GROUP,                    X
         NAME=INVDTA,                   X
         ACC=(8)
```

Group entry INVDTA allows users defined with access control class 8 to access libraries, files, or phases that begin with the character string INVDTA. Only the attempted access violations are logged.

Library Entries

```
DTSECTAB TYPE=LIB,                      X
         NAME=EMIL.PRIVATE.RELO,        X
         ACC=(1-8,32),                  X
         LOG=(1-8)
```

Library entries are used for protecting private libraries. Protecting a library means also protecting the members of that library.

Note that this entry begins with the characters EMIL, which are also defined as a group entry. The access and log specifications are a subset of that group entry. However, for access validation the library entries are searched first before the group entries. This means that users with access class 25 cannot access the library EMIL.PRIVATE.RELO, even though access is permitted at the higher EMIL group level.

File entries

```
DTSECTAB TYPE=FILE,                     X
         NAME=PAYROLL.MONTHLY,          X
         ACC=(16),                      X
         LOG=(16)
```

File entries can be used to protect DASD files and labeled tape files. The protected name is the 44-byte (DASD) or 17-byte (tape) file-ID.

Phase entries

```
DTSECTAB TYPE=PHASE,                    X
         NAME=DTSECTAB,                 X
         ACC=(16),                      X
         LOG=(16)

DTSECTAB TYPE=PHASE,                    X
         NAME=MAINT,                    X
         ACC=(9-15),                    X
         LOG=(9-15)

DTSECTAB TYPE=PHASE,                    X
         NAME=DITTO,                    X
         ACC=(9-15),                    X
         LOG=(9-15),                    X
         SUBTYPE=FINAL
```

Phase entries protect phases in the core image library. This table (DTSECTAB) itself should be protected in this way to prevent the unauthorized link-edit of the table; system programs, such as VSE/DITTO or MAINT, that can potentially bypass access control, should be protected in this manner at the program level.

SUBTYPE=FINAL must be specified for the last macro call.

For a list of security sensitive IBM programs that should be defined as protected resources, see *IBM Recommendations to Enhance Integrity* later in this chapter.

```
/*
// EXEC LNKEDT
/&
```

The macros defining the table should be written in the following sequence (with the names in collating sequence within the types) to avoid internal sort operations:

User entries
Group entries
Library entries
File entries
Phase entries

An MNOTE is issued if a SORT was necessary, so that the macros can be correctly ordered for the next generation.

To avoid possible macro generation problems, all available storage within the partition should be utilized for the assembly, that is, no SIZE parameter should be specified in the EXEC statement. If running in a VSE/ICCF interactive partition, the minimum /OPTION GETVIS=48K should be used.
The assembly can be done in a VSE/ICCF interactive partition, but the link-edit run must be executed in the BG partition. The correct phase statement is generated by the assembler with the table generation.

Protection of the Access Control Table (DTSECTAB)

To prevent manipulation and misuse of the information stored in DTSECTAB, the following precautions should be considered by the user:

- Storing the source job stream for generating DTSECTAB in the VSE/ICCF library as a protected member, allowing only the security administrator to gain access to it. (Refer also to the discussion of VSE/ICCF protection facilities in Chapter 4). A copy of the job stream should be kept as a backup version.
- Protecting the table as a phase (named DTSECTAB) in DTSECTAB as shown in the preceding example. This would allow only the installation's security administrator to access that phase.

The system scrambles sensitive information in the table to provide additional protection.

Operation with the Access Control Function

Performance Considerations

The impact on performance when using the access control function depends on how many resources are protected, how frequently they are accessed and by how many users, and whether all accesses are to be logged or only the attempted violations. It is those values that also determine the value to be specified for n in the SEC parameter of the FOPT supervisor generation macro to have a reasonable number of records to be stored in the logging queue, which allows concurrent processing of logging requests.

Shutdown of the Logging Function

If a shut-down operation is performed for VSE/ICCF, the logging function will be terminated, a message will be issued, and the log data set will be closed. Access control continues to perform its functions, but without logging access control events.

Occurrence of a Deadlock Situation

Normally, if the VSE/Access Control-Logging and Reporting program is installed, there are two logging data sets available for recording access control information. If one data set is full, the system switches to the second data set for logging the access control events. The operator is informed that the first data set should be made available again by printing the logged information or by dumping it on tape for later printing.

A deadlock situation may occur if both data sets are full (because the warning messages have been ignored), and all other partitions are waiting for logging, and no partition is free for running the reporting program. To be prepared for such a situation it might be considered to have another supervisor generated which does not support access control. However, uncontrolled usage of a supervisor without the access control support has to be prevented.

Protection of Passwords

One of the responsibilities of the security administrator is to assign the passwords and change them from time to time in order to avoid damage as a result of inadvertent or intentional disclosure.

The password itself should be composed of a random combination of alphameric characters. It should not contain any information or be mnemonic.

The system protects the password and user-ID by suppressing a display on the screen or on SYSLOG when the password or user-ID is being entered, and both are not stored on the hardcopy file.

Terminals are the preferred medium for the entry of passwords. If passwords must be included in card input, special protective measures may be required. Where possible, the password used should be that of the person submitting the card deck. Cards containing passwords should not be interpreted, and they should be destroyed as soon after use as practical. Preferably, card decks that contain passwords are to be stored on diskette.

VSE/VSAM Implications

In a system with the access control function active, the REWIND option must be specified for the particular magnetic tape volumes in the following VSE/VSAM commands: EXPORT, EXPORTRA, IMPORT, IMPORTRA, PRINT and REPRO. This means that no multifile volumes on unlabeled tapes are supported.

Tape Label Processing

In a system with the access control function active, the operator is no longer permitted to enter IGNORE as a reply to certain warning messages in order to override a label check when processing files on magnetic tape.

Auditing the Access to Controlled Resources

Auditing the access to controlled resources is a prerequisite for efficient control of an installation's sensitive data. A complete record of unauthorized attempts to access a controlled resource or, even better yet, a record of such attempts plus a list of all accesses of certain sensitive data may help the security administrator to uncover data security leaks.

The analysis of the audit trail must be carefully conducted since it helps the security administrator to

- identify access violations and the individual user accountable for it
- determine security exposures
- adjust implemented access control measures to changing conditions
- contribute to a better utilization of the system

and it may indicate the necessity of corrective action by management.

The VSE/Access Control-Logging and Reporting program, a licensed IBM program, is an efficient audit tool. Its implementation and how an audit trail is obtained are subjects discussed below.

Implementation

In order to properly execute its logging function, the above mentioned logging and reporting program requires a user to define a logging file; the log data sets. Normally, two log data sets are defined (optionally three), named IJSYSL1 and IJSYSL2. They must reside on disk, to which any programmer logical unit may be assigned. If used for the first time, the log data sets need to be initialized by running the reporting program as a normal batch job. A sample job stream (for IJSYSL1) is shown below:

```
// JOB DSPRPM INITIALIZE LOGSET
// DLBL IJSYSL1,'LOGREP.LOG.DATA.SET.1',99/365,SD
// EXTENT SYS010,DS6M31,1,1,1045,57
// ASSGN SYS010,DISK,VOL=DS6M31,SHR
// EXEC DSPRPM
          DATASET LDS=IJSYSL1
          INITIALIZE
/*
/&
```

After the VSE/ICCF partition has been started, VSE/ICCF activates the logging program, which in turn opens the log data set using the information stored in the label area during the initialization of the log data sets. If VSE/ICCF is not active, the logging program cannot be activated and no logging can be performed.

How to Get an Audit Trail

The VSE/Access Control-Logging and Reporting program enables the user, normally the security administrator, to get a printed audit trail from the information stored in the log data set. The reporting program (DSPRPM) runs as a batch job in one of the systems partitions. It produces printouts of the log data set according to the selection criteria, as defined by the user in the SELECT control statement. If a user submits a SELECT statement without a parameter, the program prints, on SYSLST, a listing of the logged events by user-ID as shown in Figure 5. However, the output of the reporting program may consist of several different reports printed on SYSLST if several SELECT control statements with different parameters are submitted.

The parameters of the SELECT control statement enable the user to determine the contents of the reports to be printed according to the existing requirements.

The following parameters are available:

BEGIN

This parameter allows the specification of date and time to determine the beginning of the selection of access control events for printing.

END

This parameter permits the specification of date and time to determine the end of the selection of access control events for printing.

USERID

This parameter allows the specification of user IDs to be selected for printing.

EVENT

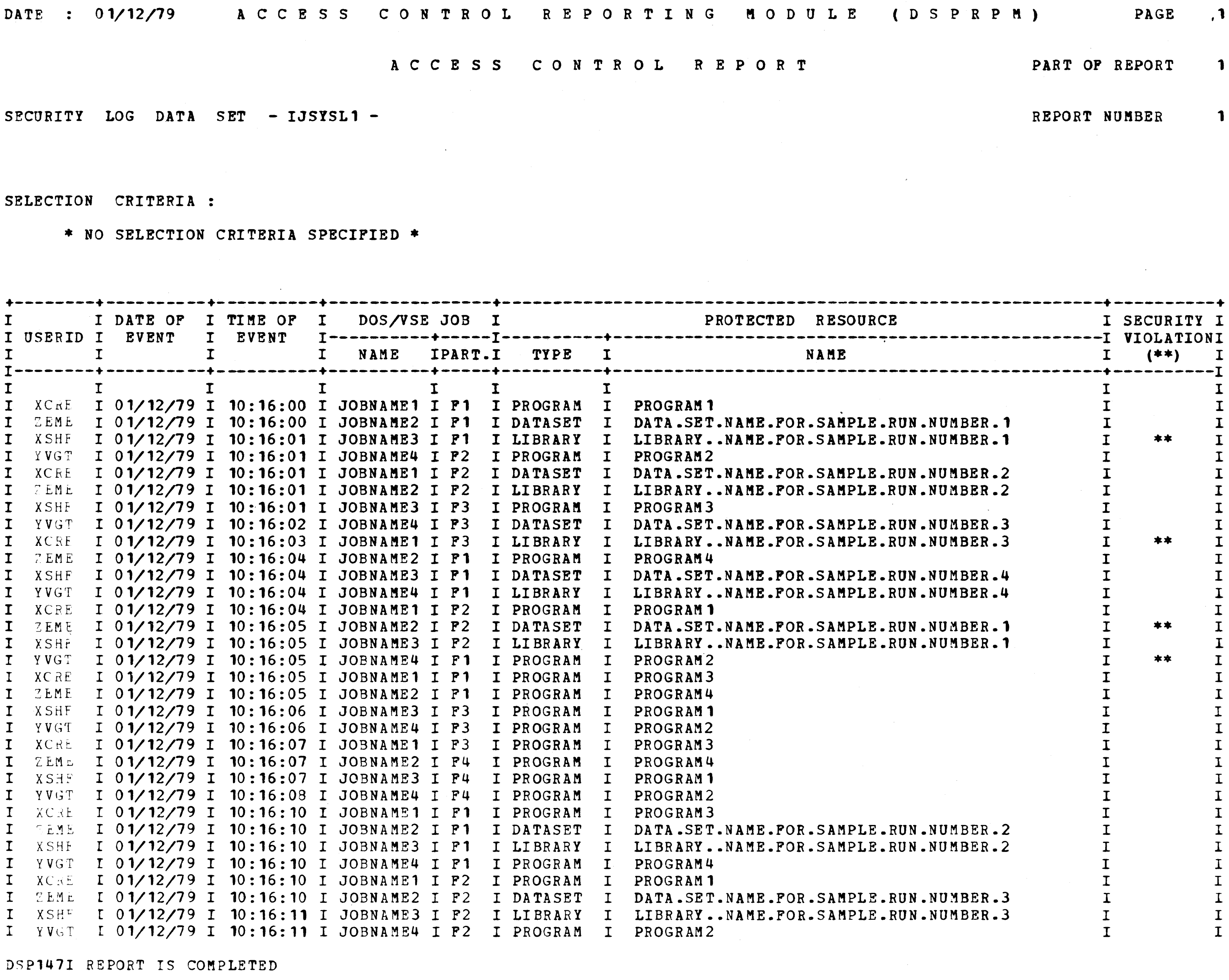
This parameter defines the type of resource for which an access control event was recorded, and which may be a phase, library, or file (data set) to be selected for printing. An access control event will not be selected for printing, if its type of event is not defined.

PGMNAME

This parameter defines the name of phases (programs) in a system or private core image library to be selected for printing.

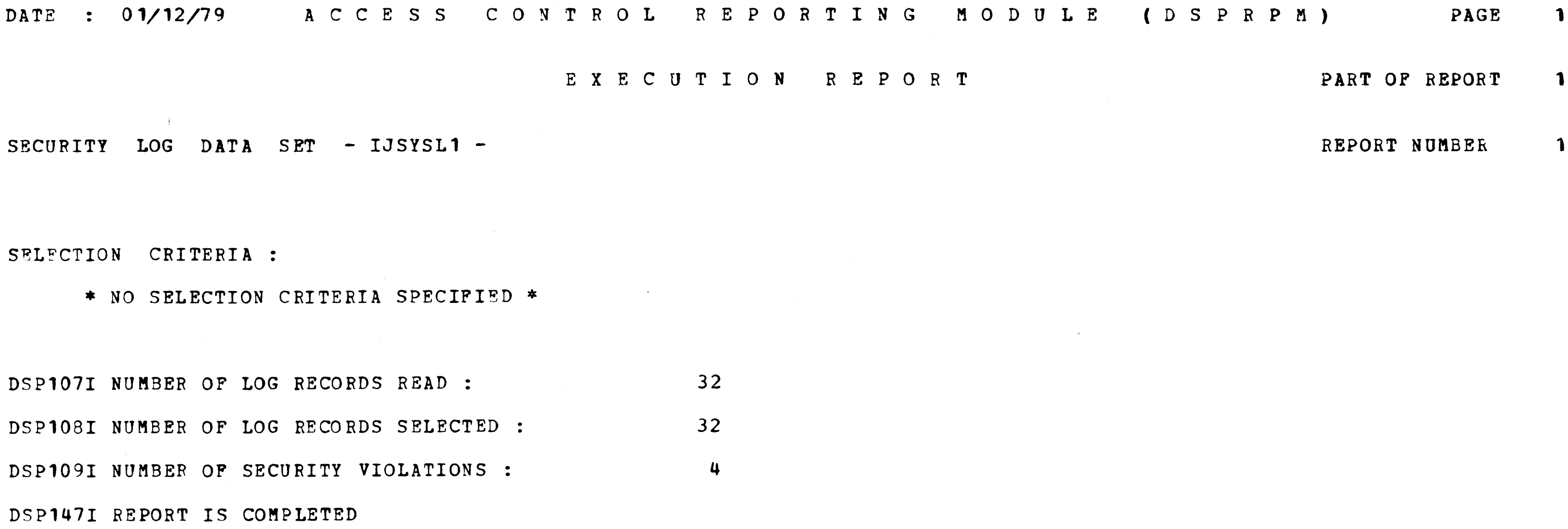
DSNAME

This parameter defines the name of files (data sets) and private libraries to be selected for printing.



```
DATE  :  01/12/79     A C C E S S   C O N T R O L   R E P O R T I N G   M O D U L E   ( D S P R P M )          PAGE    ,1

                                    A C C E S S   C O N T R O L   R E P O R T                          PART OF REPORT    1

SECURITY  LOG  DATA  SET  - IJSYSL1 -                                                                  REPORT NUMBER     1


SELECTION  CRITERIA :

     * NO SELECTION CRITERIA SPECIFIED *


+--------+----------+----------+-------------------+---------------------------------------------------------------------+----------+
I        I DATE OF  I TIME OF  I   DOS/VSE JOB     I                          PROTECTED  RESOURCE                         I SECURITY I
I USERID I  EVENT   I  EVENT   I---------+--------I----------+----------------------------------------------------------I VIOLATIONI
I        I          I          I  NAME   IPART.I   TYPE    I                         NAME                               I   (**)   I
I--------+----------+----------+---------+-----+-----------+----------------------------------------------------------+----------I
I        I          I          I         I     I           I                                                          I          I
I  XCRE  I 01/12/79 I 10:16:00 I JOBNAME1 I F1  I PROGRAM   I  PROGRAM1                                                I          I
I  ZEME  I 01/12/79 I 10:16:00 I JOBNAME2 I F1  I DATASET   I  DATA.SET.NAME.FOR.SAMPLE.RUN.NUMBER.1                   I          I
I  XSHF  I 01/12/79 I 10:16:01 I JOBNAME3 I F1  I LIBRARY   I  LIBRARY..NAME.FOR.SAMPLE.RUN.NUMBER.1                   I    **    I
I  YVGT  I 01/12/79 I 10:16:01 I JOBNAME4 I F2  I PROGRAM   I  PROGRAM2                                                I          I
I  XCRE  I 01/12/79 I 10:16:01 I JOBNAME1 I F2  I DATASET   I  DATA.SET.NAME.FOR.SAMPLE.RUN.NUMBER.2                   I          I
I  ZEME  I 01/12/79 I 10:16:01 I JOBNAME2 I F2  I LIBRARY   I  LIBRARY..NAME.FOR.SAMPLE.RUN.NUMBER.2                   I          I
I  XSHF  I 01/12/79 I 10:16:01 I JOBNAME3 I F3  I PROGRAM   I  PROGRAM3                                                I          I
I  YVGT  I 01/12/79 I 10:16:02 I JOBNAME4 I F3  I DATASET   I  DATA.SET.NAME.FOR.SAMPLE.RUN.NUMBER.3                   I          I
I  XCRE  I 01/12/79 I 10:16:03 I JOBNAME1 I F3  I LIBRARY   I  LIBRARY..NAME.FOR.SAMPLE.RUN.NUMBER.3                   I    **    I
I  ZEME  I 01/12/79 I 10:16:04 I JOBNAME2 I F1  I PROGRAM   I  PROGRAM4                                                I          I
I  XSHF  I 01/12/79 I 10:16:04 I JOBNAME3 I F1  I DATASET   I  DATA.SET.NAME.FOR.SAMPLE.RUN.NUMBER.4                   I          I
I  YVGT  I 01/12/79 I 10:16:04 I JOBNAME4 I F1  I LIBRARY   I  LIBRARY..NAME.FOR.SAMPLE.RUN.NUMBER.4                   I          I
I  XCRE  I 01/12/79 I 10:16:04 I JOBNAME1 I F2  I PROGRAM   I  PROGRAM1                                                I          I
I  ZEME  I 01/12/79 I 10:16:05 I JOBNAME2 I F2  I DATASET   I  DATA.SET.NAME.FOR.SAMPLE.RUN.NUMBER.1                   I    **    I
I  XSHF  I 01/12/79 I 10:16:05 I JOBNAME3 I F2  I LIBRARY   I  LIBRARY..NAME.FOR.SAMPLE.RUN.NUMBER.1                   I          I
I  YVGT  I 01/12/79 I 10:16:05 I JOBNAME4 I F1  I PROGRAM   I  PROGRAM2                                                I    **    I
I  XCRE  I 01/12/79 I 10:16:05 I JOBNAME1 I F1  I PROGRAM   I  PROGRAM3                                                I          I
I  ZEME  I 01/12/79 I 10:16:05 I JOBNAME2 I F1  I PROGRAM   I  PROGRAM4                                                I          I
I  XSHF  I 01/12/79 I 10:16:06 I JOBNAME3 I F3  I PROGRAM   I  PROGRAM1                                                I          I
I  YVGT  I 01/12/79 I 10:16:06 I JOBNAME4 I F3  I PROGRAM   I  PROGRAM2                                                I          I
I  XCRE  I 01/12/79 I 10:16:07 I JOBNAME1 I F3  I PROGRAM   I  PROGRAM3                                                I          I
I  ZEME  I 01/12/79 I 10:16:07 I JOBNAME2 I F4  I PROGRAM   I  PROGRAM4                                                I          I
I  XSHF  I 01/12/79 I 10:16:07 I JOBNAME3 I F4  I PROGRAM   I  PROGRAM1                                                I          I
I  YVGT  I 01/12/79 I 10:16:08 I JOBNAME4 I F4  I PROGRAM   I  PROGRAM2                                                I          I
I  XCRE  I 01/12/79 I 10:16:10 I JOBNAME1 I F1  I PROGRAM   I  PROGRAM3                                                I          I
I  ZEME  I 01/12/79 I 10:16:10 I JOBNAME2 I F1  I DATASET   I  DATA.SET.NAME.FOR.SAMPLE.RUN.NUMBER.2                   I          I
I  XSHF  I 01/12/79 I 10:16:10 I JOBNAME3 I F1  I LIBRARY   I  LIBRARY..NAME.FOR.SAMPLE.RUN.NUMBER.2                   I          I
I  YVGT  I 01/12/79 I 10:16:10 I JOBNAME4 I F1  I PROGRAM   I  PROGRAM4                                                I          I
I  XCRE  I 01/12/79 I 10:16:10 I JOBNAME1 I F2  I PROGRAM   I  PROGRAM1                                                I          I
I  ZEME  I 01/12/79 I 10:16:10 I JOBNAME2 I F2  I DATASET   I  DATA.SET.NAME.FOR.SAMPLE.RUN.NUMBER.3                   I          I
I  XSHF  I 01/12/79 I 10:16:11 I JOBNAME3 I F2  I LIBRARY   I  LIBRARY..NAME.FOR.SAMPLE.RUN.NUMBER.3                   I          I
I  YVGT  I 01/12/79 I 10:16:11 I JOBNAME4 I F2  I PROGRAM   I  PROGRAM2                                                I          I
DSP147I REPORT IS COMPLETED
```

Figure 5. Example of Print-out from the Log Data Set (Part 1 of 2)



```
DATE  :  01/12/79     ACCESS  CONTROL  REPORTING  MODULE  (DSPRPM)        PAGE    1

                                EXECUTION  REPORT                  PART OF REPORT    1

SECURITY  LOG  DATA  SET  - IJSYSL1 -                              REPORT NUMBER     1


SELECTION  CRITERIA :

      * NO SELECTION CRITERIA SPECIFIED *


DSP107I NUMBER OF LOG RECORDS READ :                  32

DSP108I NUMBER OF LOG RECORDS SELECTED :              32

DSP109I NUMBER OF SECURITY VIOLATIONS :                4

DSP147I REPORT IS COMPLETED
```

Figure 5. Example of Print-out from the Log Data Set (Part 2 of 2)

VIOLATION

This parameter determines either the printing of all previously selected access events, or only of those that constitute a violation.

SORT

This parameter permits the specification of the sequence in which the access control report is to be printed. Sort arguments may be user ID, time, or event for example. The SORT parameter requires the IBM Sort/Merge program 5746-SM2 to be installed. If the Sort/Merge program is not available, the particular SELECT control statement is not processed.

PRINT

This parameter determines either the printing of all selected events, including a summary page (execution report), or only the printing of the summary page itself.

At the end of an access control report, an execution report shows the total number of access (security) violations, for each user ID for the period of time specified in the SELECT statement, and also an indication whether or not the log data set has been cleared.

For a complete description of the VSE/Access Control-Logging and Reporting program, refer to the appropriate publications for that program listed at the end of this chapter.

Hints for Auditing

Most of the access violations originate from errors, and these frequent violations are characterized by a rather constant, average value for a given system. Each system develops such a characteristic pattern after a certain time in which the system was not subject to any changes. Any drastic deviation from such an established pattern, not resulting from changes, must be a source of alarm and needs close scrutiny.

An unusually low number of violations for example, may indicate that a way has been found to circumvent access control routines.

The following examples may illuminate the subject further:

- More people are authorized to work with the system and protected resources than are actually doing so:
  This may indicate that authorization is too easy to get without apparent necessity, or an anticipated necessity did not materialize.
- Many more authorized people work with the system and the protected resources than was anticipated:
  Again this may indicate that authorization is too easy to get, or that protection was defined for resources which actually need not be protected.

- Fewer people are authorized to use the system and protected resources than anticipated:
  This may indicate that authorization is too difficult to get, or the need to work with the system is not as high as estimated, or not all of the data that requires protected status has been defined.

- Some resources have an unexpected low access activity:
  It may indicate that the resource can possibly be removed from the system, or that an authorization is too difficult to get, or that a way has been found to circumvent protection.

- Some resources have an unexpected high access activity:
  In case of a file, it may indicate that a separation of sensitive and non-sensitive data should be considered to increase processing efficiency; for other resources, it may indicate that authorization is too easy to get.

These examples show that security measures must be reviewed frequently and be adjusted as the need arises.

The audit trail should be made available to the people and departments involved, and a list of violations should be distributed as often as possible to allow for quick reactions. A file owner, for example, should be notified if an unauthorized access to his file has been recorded.

Integrity Considerations

The VSE system is designed to protect a user or application from accidental interference by other users or applications.

Any generalized operating system, such as the VSE system, is not free from integrity exposures, and those exposures might be exploited by individuals familiar with the internals of the system.

People who deliberately use such knowledge of the internals of the system can gain unauthorized access to data and resources of the system despite of the built-in integrity safeguards. Management is responsible for introducing administrative and operational safeguards that help to avoid such exploitations and that ensure system integrity to a great extent.

To achieve an acceptable level of system integrity for a VSE installation a user should:

- Consider making the recommendations given below a part of the installation defined security procedures.

- Ensure that knowledgeable and skilled members of the installations staff will have little or no chance to access certain data or to use or manipulate certain programs. (Refer to recommendations 1 and 2.)

- Ensure that resources (mainly programs) that can be used to bypass existing integrity and security safeguards are protected properly (refer to recommendation 2.)

IBM Recommendations to Enhance Integrity

Good security practice at an installation may well require the appointment of one person who is responsible for establishing and enforcing security procedures. The role of this person - the installation's security administrator - is discussed further following the IBM recommendations. For a VSE system these recommendations are:

1. Good security practice requires that the ability to modify the operating system should be restricted to only a few and trusted individuals and a change should be controlled by management.

2. Only one or few persons should be allowed to use the programs listed below, since they may enable a user to circumvent existing safeguards with the intent of accessing protected data, or running programs for his own benefit, or he may be destroying important data. Therefore, these programs should be individually protected, for example by assigning a specific access control class when having the access control function of the VSE system installed. The programs are:

   Assembler (ASSEMBLY)
   Linkage editor (LNKEDT)
   Data interfile transfer, testing and operations utility (VSE/DITTO)
   Library organization program (CORGZ)
   Core image library patch program (PDZAP)
   Library maintenance program (MAINT)
   Maintain system history program (MSHP)
   Dump utility program (DOSVSDMP)
   VSE/VSAM service programs (IKQVEDA, IKQVDU, and IDCAMS)
   Library services (CSERV, RSERV, SSERV, PSERV)
   Fast copy data set (FCOPY, FCOPYFB)
   Initialize tape (INTTP)
   Initialize disk (INTDK)
   Clear disk (CLRDK)
   VTOC display (LVTOC)
   Backup system (BACKUP)
   Restore system (RESTORE)
   Device support facility (ICKDSF)

   The DOSVSDMP generated stand-alone dump program should be kept under lock and key by the security administrator; the same is true for the stand-alone program Fast Copy Disk, and the stand-alone versions of Initialize Disk and Restore System.

3. The DASDFP file protection feature should be used (DASDFP system generation option) to ensure that data is not written outside the limits of a DASD file currently being processed.

4. When using the access control function of the VSE system, group names should be used to protect files immediately after they have been created.

5. When using the access control function of the VSE system, VSE/VSAM should be used as an access method to control adequately the access to files on a read/update level.

6. The security administrator may consider defining in the installation's security procedures that NODUMP has to be specified in the // OPTION statement for those programs which process sensitive data, so as to avoid having such data become exposed in case of a cancel situation.

The Security Administrator

A security administrator at a VSE installation just cannot fully discharge his responsibilities without the support of adequate software facilities. A person appointed to assume the responsibility of safeguarding an installation's assets (data and programs) should therefore carefully review the available standard facilities in support of operating system integrity as well as the capabilities of the access control function of the VSE system. A security administrator should do this review in full consideration of the various responsibilities that a person in such a position normally must assume, some of which are indicated below:

- Together with management, prepare a list of sensitive files and of programs that process these files.
- Determine who of the installation's staff is authorized to use those programs and establish procedures that ensure that authorized persons only, and no one else, will be able to invoke the programs.
- Ensure that none of the installation's staff catalogs, in the operating system's libraries, a program that accesses sensitive data without authorization.
- Minimize the chance that unauthorized access of sensitive data remains undetected.

While proper usage of the standard integrity facilities might suffice for a small VSE installation with only one or two sensitive files or programs, it is obvious that larger installations with numerous sensitive files and associated programs need more efficient software support. The access control function of the VSE system might well answer that installation's security requirements.

Related Publications

The following publications provide additional information for the topics discussed in this chapter:

VSE/Advanced Functions System Management Guide, SC33-6094
VSE/Advanced Functions System Control Statements, SC33-6095
VSE/Advanced Functions Macro User's Guide, SC24-5210
VSE/Advanced Functions Macro Reference, SC24-5211
VSE/Advanced Functions System Generation, SC33-6096

VSE/Interactive Computing and Control Facility:
General Information Manual, GC33-6066
* *Installation and Operations Reference,* SC33-6067
* *Terminal Users Guide,* SC33-6068

VSE/Access Control-Logging and Reporting:
General Information Manual, GH12-5130
* *Program Reference and Operations Manual,* SH12-5336

* Normally available only if the particular licensed IBM program has been installed.

Chapter 4: Protection Facilities Available with Optional Program Products

This chapter introduces data protection facilities of a number of program products, frequently used with the VSE system:

VSE/POWER
VSE/VSAM
VSE/ICCF
CICS/VS
DL/I DOS/VS

Their protection capabilities may be used separately or in addition to complement existing data security arrangements. Whenever working with such a component or subsystem, it must be ensured that the information which determines the data protection capabilities (passwords, security classes for example), can be accessed by the security administrator only. Utilities and programs that serve to generate and update tables and profiles containing protection information should only be accessible to the security administrator.
Programs that may be misused to acquire information serving protection purposes must be protected accordingly, to allow only authorized users to access them.

VSE/POWER

VSE/POWER has been designed to improve the throughput of a computing system by separating unit-record input and output operations by reading card or diskette input, and writing this input onto disk from where this input is made available to the appropriate problem programs, and by writing punched card and printed output onto disk or magnetic tape from where this output is punched or printed or both.

Reader Exit

When VSE/POWER is generated, the parameter RDREXIT permits the specification of a user-written reader exit routine.

After the initialization of VSE/POWER, the phase with the name specified in the RDREXIT parameter is loaded into the VSE/POWER partition. The phase receives control from VSE/POWER for any job control or VSE/POWER JECL statement that is being read.

Any job control or JECL statement can be changed or deleted, and other statements can be inserted. An attempted access violation may thus be detected and indicated by the insertion of a comment; this is shown by the example below.

Original job stream:

```
// JOB PAYROLL
// ASSGN ...
// EXEC PAYROLL1      CODE=WRONG
/&
```

Job stream as listed after processing:

```
// JOB PAYROLL
// ASSGN...
* ACCESS VIOLATION   PGRM=PAYROLL1
// EXEC NOT ALLOWED
/&
```

The following statements are processed:

```
//
$$
/*
/&
*
```

This means that certain statements, for example permanent assignments (ASSGN ...), are not processed by a VSE/POWER exit routine. The job control exit, and the VSE/POWER reader exit work independently of each other. The VSE/POWER reader exit is activated before the job control exit, and the processing of the various statements must be distributed reasonably if both exits are used side by side.

An exchange of information between the two exits is only possible if the VSE/POWER exit routine stores the information in the appropriate job control statements.

The VSE/POWER reader exit does not process job control statements of procedures, or the SLI (Source Statement Library Inclusion), since those statements are read directly from the libraries at processing time. This is also true for the VSE/POWER spool macros and the internal reader facility. A checking of statements submitted in such a way must be handled by the job control user exit routine.

RJE User Identification

When an RJE environment is generated a password can be specified in the PLINE macro (which defines the hardware characteristics of an RJE/BSC line), the PRMT macro (it defines the hardware characteristics of an RJE terminal), and in the SNA parameter of the VSE/POWER generation macro for the RJE/SNA support.

Whenever the remote operator wants to connect his terminal to the central system (SIGNON/LOGON), he has to submit the generated password. If the submitted password does not agree with the password specified at the time of RJE generation, the SIGNON/LOGON procedure is canceled.

The following rules should be observed when installing an RJE environment:

- All RJE devices should be attended. Unattended devices are appropriate only to 'open-shop' operation. Exceptions to this rule require the implementation of access control software at the central computer site, such as the access control function of the VSE system (refer to Chapter 3).
- Terminal operators should ensure that all jobs meet installation rules and are properly identified with the submitter.
- Operators should ensure that output is returned only to the individual indicated by the output statement.
- All resource usage or access should be journaled and properly accounted for.

VSE/VSAM

VSE/VSAM is an access method that creates, maintains and processes files on direct access storage devices. VSE/VSAM offers a set of options to support data protection. In the DEFINE command the following data protection related parameters can be specified:

READPW	Read password
UPDATEPW	Write password
CONTROLPW	Control password
MASTERPW	Master password
ATTEMPTS	Number of attempts for supplying the password
CODE	Cover name with which the operator is prompted to supply the password
AUTHORIZATION	User exit
OWNER	Owner identification
FOR | TO	Retention period
SHAREOPTIONS	Resource sharing
ERASE | NOERASE	Optional data deletion

Passwords to Authorize Access

Passwords can be defined to authorize access to clusters (data and index), alternate indexes, and catalogs.

- Read access (READPW parameter). This password authorizes the user to retrieve data records or catalog entries.
- Update access (UPDATEPW parameter). This password authorizes a user to retrieve, update, add, or delete records in a file; if defined for a catalog, the password authorizes a user to define files in that catalog.
- Control-interval access (CONTROLPW parameter). This password authorizes a user to use control-interval access.

- Full access (MASTERPW parameter). The master password authorizes a user to perform all operations (retrieving, updating, adding and deleting) on a file, on a catalog, or any index associated with a file.

Catalogs, which describe the VSE/VSAM files, are VSE/VSAM files themselves and may have passwords. If passwords are defined for files in a catalog, passwords must also be defined for the catalog, in order to have effective file passwords.

The password is normally supplied by the program, or through VSE/VSAM parameters, or by the operator. If a wrong password is supplied, OPEN processing is terminated.

The ATTEMPTS parameter (a value from 0 to 7) allows to specify the number of times the operator can attempt to supply the correct password. The default value is 2.

The CODE parameter allows to specify a 1 to 8 character name, serving as a cover name for the 44-byte file-id of the DLBL statement, to which the operator responds with the password. This prompting code prevents the operator from knowing both, the password and the file-id of a file.

User Security Verification Routine

The AUTHORIZATION parameter serves to define a user-written security verification routine (USVR). This routine, if present, receives control whenever an attempt was made to open a VSE/VSAM component, or access its catalog entry, and no password or a password other than the appropriate master password was supplied. The parameter list provided by VSE/VSAM for the USVR routine contains, among other information for security checking, the 44-byte file-id, the OWNER identification, and the password.

When the routine returns control, it must indicate to VSE/VSAM whether or not the requested access is permitted.

Protecting Shared Data

Files can be shared among partitions, or among tasks in a partition. The level of sharing is defined in the SHAREOPTIONS parameter. Four share options are available.

If the file to be accessed cannot be shared for the specified type of processing, no OPEN can be performed.

Retention Period

The FOR parameter specifies the number of days for which the data is to be retained.

The TO parameter specifies the date through which the data is to be retained.

Optional Data Deletion

The ERASE parameter specifies whether a data component is to be erased (to be overwritten with binary zeros), when its entry in the catalog is deleted.

Recommendations

When working with VSE/VSAM, the following recommendations should be observed:

- Access to all catalogs and most files should be restricted to the smallest set of people consistent with system objectives.
- Passwords should be known by as few people as possible.
- Each file should have its own READ, UPDATE and CONTROL passwords. Each of these passwords should be different.
- Only one person should know the UPDATE password for a particular file.
- There should be a limited number of MASTER passwords (each covering multiple files). These passwords should each be held by no more than two people.

VSE/Interactive Computing and Control Facility (VSE/ICCF)

VSE/ICCF is designed to provide the processing power of the computer to several terminal users on a time shared basis and to allow the users to work with the computer simultaneously in the form of some kind of a dialogue. VSE/ICCF offers extensive data protection features as required for a time sharing system.

Data protection is achieved through:

- user profiles
- libraries
- alternate security option
- data protection tables
- user control

User Profiles

Each user is defined to VSE/ICCF by a unique, four character user identification code (user-ID). Associated with the user-ID is an 80-character data record, the user profile record. This record contains information such as the associated password and security class, and thus defines which data the user is authorized to access; the record also supplies user-related processing information.

User-ID

The user-ID must be supplied during the log-on procedure, and ~~no~~ user is logged on to the system without having entered a user-ID that is known to the system. The user-ID enables the system to search for the appropriate user profile record; it is also used to provide protection for data members, when several user-IDs are associated with a given library.

Log-on Password

During the log-on procedure, a three to six character password must be supplied to VSE/ICCF for authentication purposes. This password must match with the one that is stored in the user's profile record. If the password does not match, the user is not logged-on to the system. To provide continuing protection, the password should be altered by the security administrator from time to time.

Security Class

The security class defines which programs in the core image library, and which files and disk volumes of the system a VSE/ICCF user is authorized to access for processing in a VSE/ICCF interactive partition. For a user's profile record, up to 32 security classes may be defined.

Libraries

Different types of libraries and data definitions provide for data protection within the VSE/ICCF environment. The following libraries and data definitions can be specified:

Libraries	Data
Public/Private	Public/Private
Shared/Owned	Common
Alternate	
Common	

Public and Private Libraries

A public library can be accessed by any VSE/ICCF user; a private library only by a user who is authorized by an appropriate entry in his user profile record.

Shared and Owned Libraries

An owned private library provides for the highest level of data protection since only the owner can access such a library. A shared private library may be used by two or more users, if the data has been entered as public. The user of a shared private library can secure his data by entering it as private or with member password protection (see also *Member Password* below).

Alternate Library

A user always has one main library. This library may be owned or shared, and it may be the only library to which the user has access. However, it is possible to specify, in a users profile record, up to eight alternate private libraries that may be owned or shared with other users.

After logging on to the system, only the main library is accessible. By the use of a command, a user can switch from one library to another as long as the library he is switching to is a public library, or has been specified in his profile record as an alternate private library.

Public and Private Data

All data saved in a library is entered as public or private. If neither is specified, the default is found in the user's profile record. Public data may be accessed by any user who shares the library.

Private data may be read by any user who shares the library, but modified only be the user (user-ID) who entered the data.

Member Password

A user can protect his data members in the library with a four character password. If the member is flagged as private, only the user entering the data can modify it; if the member is flagged as public, any user having access to the given library and knowing the password may modify the particular data.

Common Library Members and Common Data

To have library members or data universally accessible to all terminal users, such library members or data may be defined as 'common'.

Common Library Members

To avoid that all common members are represented in each directory, a common library may be installed.

If a desired member name is not found in the user's main library, or a connected library, the common library directory will be searched for the member name as well.

Common Data

Common data refers to data members which exist only once within the entire library. However, each data member appears as a directory entry in every user's library.

This data is usually reserved for common subroutines or for procedures generally applicable. Common data is public data in the sense that all users have access to it. However, only the central site may update the data.

Alternate Security

The VSE/ICCF time sharing system may be implemented with the alternate security option. This means that public data can be read by any user, but updated only by the user who entered the data, and that private data can be accessed only by the user who entered the data.

Data Protection Tables

To protect system resources, such as programs, files and volumes, they have to be defined for inclusion in the appropriate table with applicable use classifications assigned. VSE/ICCF maintains three tables:

- System Program Table
- Load Protection Table
- System File Table

System Program Table

This table contains entries of programs (compilers, utilities and application programs), which define certain use classifications assigned to a program. For protection purposes, programs can be classified as authorized only, or they can be assigned a security class or both. Programs specified as authorized are accessible to authorized users only. To execute such a program, the user must have set the authorized user flag in his profile record. Candidates for an authorized-only classification are programs such as VSE/DITTO, the assembler, or MAINT, that might prove too prone to abuse by certain terminal users.

If the security class assigned to a program does not agree with the security class of the user, no access is allowed to the program. For example, if the program is protected with SEC=(1,12,20), the program can only be executed by a user who has been specified with at least one of the three security classes 1, 12, or 20. A total of 32 security classes is available.

Load Protection Table

This table is part of the optional load protection feature, and defines core image library phases or groups of phases to be protected against access by LOAD/FETCH SVC's issued by other programs.

The load protection table complements the system program table, which provides for checking only the first phase loaded by the /LOAD job entry statement in a job step.

System File Table

The system file table contains entries that specify disk volumes and files. For protection purposes access to files and volumes can be restricted to users with the authorized-only classification assigned to, or users of a given security class (32 security classes are available).

User Control

VSE/ICCF records processing information on a user basis such as command and data entries, system responses, user-IDs, number of log-on's, and the number of program executions. This information can be used to control and supervise the system and its use.

VSE/ICCF Access Control versus System Access Control

If the supervisor has been generated with SEC=NO, VSE/ICCF uses its system program, load protection, and system file tables for the checking of access authorization when a VSE/ICCF user accesses resources defined in those tables for processing in an interactive partition.

If the supervisor has been generated with SEC=n, the three tables are ignored for the access authorization checking as described above (but are needed for other types of processing by VSE/ICCF), since the access authorization checking for resources is done by using the access control table DTSECTAB generated for the system's access control function (the access request may originate from a VSE/ICCF user or a batch job). Therefore, for a system with SEC=n, all resources to be protected must be specified in DTSECTAB.

Refer to Chapter 3 for a description of the access control function of the VSE system.

CICS/VS

The Customer Information Control System/Virtual Storage (CICS/VS) controls on-line DB/DC applications. The following paragraphs discuss the data protection facilities available with CICS/VS.

Sign-on Procedure and Sign-on Table

A user who wants to work with CICS/VS can only do so after a successful sign-on procedure, during which the user has to supply his user-ID and password. Only if the user-ID is known to the system and the password supplied correct, is the user allowed to proceed.

User-ID and password are internally stored in the sign-on table, which also contains one or more security keys for each user. CICS/VS provides up to 24 security keys.

Program Access Control

To start processing after sign-on, the user has to specify a translation identification code (up to four characters), which invokes the appropriate application program. All transactions (programs) allowed to be processed, are defined in the Program Control Table (PCT), and each transaction can be given a security key (a number from 1 to 24). Only if the security key of the transaction being initiated matches with one of the user's security keys does CICS/VS allow processing to take place. If the security keys do not match, a message is issued to the user and also to the operator at the master terminal, identifying the terminal and the user who attempted to initiate the transaction without authorization either by mistake or on purpose.

Data Integrity Facilities

Data integrity is supported by a technique that prevents the loss of information, if two or more users try to update the same data at the same time. CICS/VS ensures that updating requested by one user is completed before updating by another user can start.

Another feature ensures that, in case of a transaction failure, all updates performed so far are canceled to prevent other transactions from using erroneous data.

Statistics allow to control and supervise the activities at the terminals.

DL/I DOS/VS

The Data Language/I Disk Operating System/Virtual Storage (DL/I DOS/VS), is a data management control system that assists the user in implementing data base processing applications. The following paragraphs discuss the data protection facilities available with DL/I.

VSE/VSAM Password Protection

Since DL/I uses VSE/VSAM as an access method, the VSE/VSAM password protection feature is available also to DL/I users. DL/I accesses VSE/VSAM files in the control interval mode. This requires to specify the VSE/VSAM password CONTROLPW for password protection. The password cannot be specified in the program, since the VSE/VSAM Access Control Block (ACB) is not accessible to a DL/I program; it must be supplied through VSE/VSAM parameters, or by the operator. Refer also to the VSE/VSAM section in this chapter.

Data Base Sensitivity

The data base segments which a specific application program is permitted to access are defined in the Program Specification Block (PSB), which is separated from the application program. A segment can be accessed by an application program only if that segment has been defined in the program's PSB. Access authorization can be further restricted to individual fields, that is, an application program may be authorized to access only certain fields of a segment. This concept of segment and field level sensitivity provides for centralized control over the access to the data base.

The processing options of an application program can also be restricted. To prevent erroneous updating, updating can be restricted to one or two programs, allowing the other programs only to access the data base for retrieval.

Protection can be further enhanced if the PSB's and DBD's (Data Base Definitions) are centrally maintained by only one person: the data base administrator.

Data Encoding

DL/I provides an exit, available with variable length records, for encoding/decoding data through a user-supplied routine. This feature may be useful for protecting externally stored data during transport. The feature can also be used for data compression.

Program Isolation and Multi-Partition Support

Both features enhance data integrity. Program isolation ensures, in case of on-line data base processing, that a segment is accessible for updating by only one task at a time.

Multi-partition support allows to access a data base from an on-line partition (CICS/VS), and a batch partition concurrently. It is achieved by having all accesses, including those from the batch partition, controlled by CICS/VS.

Related Publications

The following publications provide further information for the topics covered in this chapter:

VSE System Data Management Concepts, GC24-5209

* *VSE/POWER Installation and Operations Guide,* SH12-5329
* *VSE/POWER Remote Job Entry User's Guide,* SH12-5328

VSE/VSAM General Information, GC24-5143
* *VSE/VSAM Commands and Macros,* SC24-5144
* *VSE/VSAM Programmers Reference,* SC24-5145

VSE/Interactive Computing and Control Facility:
General Information Manual, GC33-6066
* *Installation and Operations Reference,* SC33-6067
* *Terminal User's Guide,* SC33-6068
* *Messages,* SC33-6069

Customer Information Control System/Virtual Storage (CICS/VS):
General Information, GC33-0066
* *System Programmers Guide (DOS/VS),* SC33-0070
* *System/Applications Design Guide,* SC33-0068
* *Application Programmer's Reference Manual:*
Command Level, SC33-0077
Macro Level, SC33-0079
* *Subset User's Guide (DOS/VS),* SC33-0082
* *Operators Guide,* SC33-0080

Data Language/I Disk Operating System/Virtual Storage (DL/I DOS/VS):
General Information, GH20-1246
* *Application Programming Reference Manual,* SH12-5411
* *System/Application Design Guide,* SH12-5413
* *Utilities and Guide for the System Programmer,* SH12-5412
* *Operator's Reference Manual and Messages and Codes,* SH12-5414

* Normally available only if the particular licensed IBM program has been installed.

Appendix: Description and Format of Macro DTSECTAB

Macro DTSECTAB has the following format:

```
DTSECTAB
         TYPE=USER | GROUP | LIB | FILE | PHASE,
         NAME=username | groupname | libname | filename | phasename
         [,PASSWRD=password]
         [,AUTH=YES | NO]
         [,ACC=(class, class, ... U)]
         [,LOG=(class,class,...]
         [,SUBTYPE=INITIAL | FINAL]
```

TYPE

Defines either a user or a resource profile entry. A resource may be specified as GROUP, (to protect a group of resources), LIB (to protect a library), FILE (to protect a file), or PHASE (to protect a phase/program).

NAME

Defines the name of a user, or of a resource to be protected.

If TYPE=USER, the user name is a 4 character user ID required for the identification procedure.

If TYPE=GROUP the 1 to 7 character group name allows to cover a number of resources for the access authorization validation. For example, if 'PAYROLL' is specified as a group name, then all library, file and phase (program) names beginning with 'PAYROLL' would be protected, according to the security classes defined for the group name 'PAYROLL'.

This is a useful method for securing a group of resources, and, at the same time, minimizing the table size. The table is always searched for group entries after the library, file, or phase entries.

Note: This parameter allows the protection of newly created resources, not yet protected individually by a table entry.

If TYPE=LIB, the library name is the 1 to 44 byte file identification as it is stored in the VTOC of a disk volume.

If TYPE=FILE, the file name is the 1 to 44 byte file identification as it is stored in the VTOC of a disk volume, or the 17 byte tape ID, in case of a tape file.

If TYPE=PHASE, the phase name is a 1 to 8 byte name of a phase in the core image library.

PASSWRD (only applicable if TYPE=USER)

Specifies a 3 to 6 character password associated with the specified user and is required for the authentication procedure.

AUTH (only applicable if TYPE=USER)

This authorization parameter identifies the user as the security administrator, and only one such entry is allowed in the table. This user (the security administrator) has access to all secured resources without restrictions, and must be defined by specifying YES. NO is the default.

ACC

Defines 1 to 32 access control classes to control the access to a file, library or phase. For example, if ACC=(5, 7, 8-10) is specified for a resource, only users defined with at least one of the access control classes listed above can access this resource.

For user entries only:

The option U (which stands for update) is available for user entries only. For example, ACC=(5, 7, 8-10, U) indicates that the user has read-only authorization for security classes 5 and 7, and update authorization for the resources defined with one or more of the access control classes 8-10.

Note: A read-only authorization provides for acceptable update (write) protection only if the particular resource is a VSE/VSAM file. Therefore, non-VSE/VSAM files and libraries should be defined with update authorization in the user entries.

LOG (only applicable if TYPE=GROUP or LIB or FILE or PHASE)

This option allows to define logging classes, in the same way as the access classes above. The logging option serves to determine whether all accesses of a certain access class to a resource are logged, and is only meaningful if it corresponds to one or more access classes specified for the resource. If the logging option is not specified for a specific access class only the attempted access violations, but not the allowed accesses to a resource, are logged.

SUBTYPE

The first macro call in the job stream must indicate INITIAL as a SUBTYPE, and the last macro call must indicate FINAL.

Index

GC33-6077-1

Data Security Under the VSE System (File No. S370/4300-20) Printed in U.S.A. GC33-6077-1

IBM®

International Business Machines Corporation
Data Processing Division
1133 Westchester Avenue, White Plains, N.Y. 10604

IBM World Trade Americas/Far East Corporation
Town of Mount Pleasant, Route 9, North Tarrytown, N.Y., U.S.A 10591

IBM World Trade Europe/Middle East/Africa Corporation
360 Hamilton Avenue, White Plains, N.Y., U.S.A. 10601

READER'S
COMMENT
FORM

Data Security
Under the VSE System
Order No. GC33-6077-1

This manual is part of a library that serves as a reference source for system analysts, programmers, and operators of IBM systems. This form may be used to communicate your views about this publication. They will be sent to the author's department for whatever review and action, if any, is deemed appropriate. Comments may be written in your own language; use of English is not required.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation whatever. You may, of course, continue to use the information you supply.

Note: *Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.*

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name and mailing address:

____
____
____

What is your occupation?______________________________

Number of latest Newsletter associated with this publication:____________________

Thank you for your cooperation. No postage stamp is necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Note: Staples can cause prob[illegible] with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

GC33-6077-1

--Cut or Fold Along Line--

Reader's Comment Form

Fold and tape | Please Do Not Staple | Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 40 ARMONK, N.Y.

POSTAGE WILL BE PAID BY ADDRESSEE:

International Business Machines Corporation
Department 812 BP
1133 Westchester Avenue
White Plains, New York 10604

Fold and tape | Please Do Not Staple | Fold and tape

IBM®

International Business Machines Corporation
Data Processing Division
1133 Westchester Avenue, White Plains, N.Y. 10604

IBM World Trade Americas/Far East Corporation
Town of Mount Pleasant, Route 9, North Tarrytown, N.Y., U.S.A 10591

IBM World Trade Europe/Middle East/Africa Corporation
360 Hamilton Avenue, White Plains, N.Y., U.S.A. 10601

Data Security Under the VSE System (File No. S370/4300-20) Printed in U.S.A. GC33-6077-1

GC33-6077-1

Data Security Under the VSE System (File No. S370/4300-20) Printed in U.S.A. GC33-6077-1

IBM®

International Business Machines Corporation
Data Processing Division
1133 Westchester Avenue, White Plains, N.Y. 10604

IBM World Trade Americas/Far East Corporation
Town of Mount Pleasant, Route 9, North Tarrytown, N.Y., U.S.A 10591

IBM World Trade Europe/Middle East/Africa Corporation
360 Hamilton Avenue, White Plains, N.Y., U.S.A. 10601