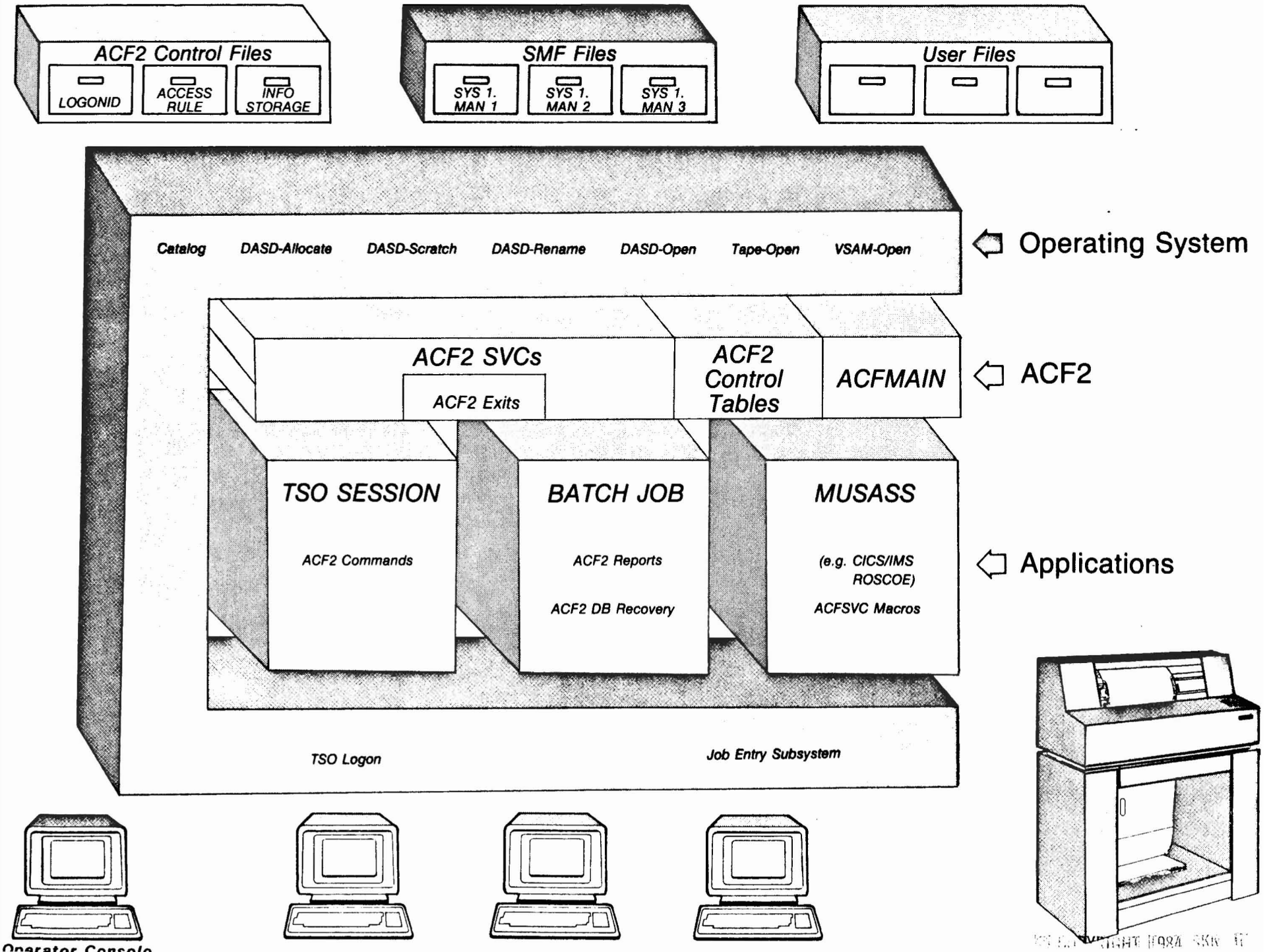
MAJOR COMPONENTS OF AN ACF2-PROTECTED SYSTEM



MAJOR COMPONENTS OF AN ACF2-PROTECTED SYSTEM

Introduction

The accompanying chart and the text that follows represent a simplified "big picture" of the ACF2 product and its environment. They are intended to be used as an introduction to the components and processing of the ACF2 system.

ACF2 Control Files

There are three control files in ACF2: the Logonid Database, the Access Rule Database, and the Information Storage Database.

The Logonid Database defines system users. An installation inserts one record per user into this control file to specify each person's privileges, attributes, and authorities. At the time of system access, the user's record is brought into storage for ACF2 user authentication through password matching, and for identification of special privileges (e.g., whether this is a security officer). Additional fields in this record are checked to see if they point to records on the Information Storage Database that define source, shift (time-of-day), or scopelist (extent of authorities) restrictions for this user.

The Access Rule Database contains records that allow for the controlled sharing of data. One record (called a "ruleset") is inserted per dataset high-level index to define the sharing conditions for all datasets beginning with that high-level index. When a user accesses data that he does not own (ownership is defined by a field called "PREFIX" in the Logonid record), ACF2 interrogates the ruleset for this high-level index to see if the user is allowed the type of access he is requesting (READ, WRITE, ALLOCATE, or EXECUTE) for the dataset in question. Additional fields in this record could point to records on the Information Storage Database that provide source or shift (time-of-day) definitions for the use of this dataset.

The Information Storage Database is used for a variety of purposes. Some records identify which days, dates, and times constitute a shift as referenced in a Logonid or rule record. Other records identify which terminals constitute a given group of input sources as named in a Logonid or rule record. Still others identify the scope of a privileged user (e.g., what high-level indices a security officer can write rules for).

Finally, the Information Storage Database contains a class of records called generalized resource rules. These records define the sharing conditions for logical resource types such as TSO account numbers, CICS transactions, IMS transactions, or any other resouce that an installation wants to define locally. One record (called a "ruleset") is inserted per resource and type combination to define the sharing conditions for that resource. When a user requests a resource within one of these protected types, ACF2 interrogates the "ruleset" record for that specific resource to see if the user is allowed access. For example, for the use of a particular transaction in IMS, the resource rule record associated with the actual transaction id would be interrogated. Additional fields in this record could point to other records on the Information Storage Database that provide source or shift (time-of-day) definitions for the use of this logical resource.

SMF Files

The System Management Facility files contain data gathered by the operating system (MVS or VS1) to provide information about the computer's usage.

Whenever ACF2 writes a record to one of its control files, it writes a duplicate record to SMF. These records act as input to ACF2 report programs that print audit trails of control file changes. These records also act as input to the ACF2 recovery program that can reconstruct a control file, should it become unusable.

Other records are added to the SMF files by ACF2 when an attempted access violation occurs or when a logging or trace of an access has been requested. These records serve as input to other ACF2 report programs.

User Files

User files represent application datasets and program libraries that ACF2 is to protect. Ownership should be defined and access rules should be written not only for these but also for system files and databases (e.g., the SMF files and system libraries).

Operating System

MVS and VS1 are operating systems that perform many functions for users. With or without ACF2 installed, they process jobs and prepare datasets for use. With ACF2 installed, these system functions are not altered or replaced, but they have been "front-ended" or intercepted by ACF2. The purpose of the ACF2 "front ends" is to call the ACF2 SVCs (system routines) to check resource authorization. If a user is not explicitly allowed access to a resource, ACF2 will prevent the access. Otherwise, the ACF2 intercepts will pass control back to the operating system to complete authorized functions as normal. The operating system is basically unaware that ACF2 has performed a validation.

Two of the operating system intercepts are involved in validating access to the use of the computer system itself. The job entry subsystem (JES, JES2, or JES3) modifications call the ACF2 SVCs to authenticate the user's identity and determine if he is authorized to run batch jobs. The TSO logon intercept calls the ACF2 SVCs to authenticate the user's identity and determine if he is authorized to access the MVS time sharing option (TSO).

The catalog, DASD-allocate, DASD-scratch, DASD-rename, DASD-open, tape-open, and VSAM-open "front ends" are among the ACF2 intercepts that call the ACF2 SVCs to determine if a user is authorized to access particular datasets in particular ways (READ, WRITE, ALLOCATE, or EXECUTE).

ACF2

The heart of ACF2 consists of ACF2 SVCs, ACF2 Control Tables, and ACFMAIN.

The ACF2 SVCs perform the bulk of ACF2's processing. Supervisor calls (SVCs) are functions, performed by the operating system or extensions to it, which can be directly invoked from a program. Common examples of operating system SVCs are dataset open and dataset close.

ACF2 acts as an extension to the operating system by adding two supervisor calls which perform logon validation, access rule validation, resource rule validation, and ACF2 control file manipulation (the adding, deleting, modifying, or retrieving of records).

ACF2 Exits are optional user written routines that are invoked by ACF2 before and/or after the SVCs are invoked. This allows an installation with unique requirements to write code to augment or tailor ACF2's processing to meet its special needs.

ACF2 also has in-storage Control Tables. The major one specifies system options and records system status. It is built from the ACF2 Field Definition Record and, among other things, specifies what mode ACF2 is in (QUIET, LOG, WARN, RULE, or ABORT), what DASD and tape volumes ACF2 is to protect, and what fields make up each Logonid record in the Logonid Database. Other tables are used for performance and for recording of transitory information.

ACFMAIN is the task that initializes ACF2 by opening the three control files and building the control tables. After that, it has two primary responsibilities. First, it handles operator console modify commands, such as to rebuild a particular control table. Second, it initiates daily backups of the three control files.

Applications

When a user starts a TSO session by logging-on, ACF2 intercepts the request and calls the ACF2 SVCs to retrieve the user's Logonid record from the Logonid Database and place it in storage. If user authentication and identification complete sucessfully, ACF2 passes control to normal TSO processing; otherwise ACF2 aborts the request.

If the user tries to access a dataset, a "front-end" again intercepts the request, calls the ACF2 SVCs to validate the request, and then aborts the request if the user is not authorized, or returns control to the operating system to complete the request if the user is authorized.

Finally, the ACF2 system provides TSO commands that can be used to administer or maintain the three ACF2 control files. These commands invoke the ACF2 SVCs to add, modify, list, or delete records on the Logonid, Access Rule, or Information Storage Databases. Before the ACF2 SVCs process a request, they make sure the user has the appropriate authority (SECURITY, ACCOUNT, LEADER, CONSULT, or USER) and is operating within his scope of responsibility. It should be noted that these commands can be executed in batch or through SPF panels and CLISTs, as well as through native TSO.

For batch jobs, modifications in the job entry system (JES, JES2, or JES3) scan the JCL for Logonids and passwords, and call the ACF2 SVCs to perform Logonid validation.

If a job tries to access a dataset, an operating system "front-end" (e.g., DASD-open, VSAM-open, or tape-open) intercepts the request, calls the ACF2 SVCs to validate the request, and then aborts the request if the user is not authorized, or returns control to the operating system to complete the request if the user is authorized.

ACF2 includes report programs, normally run daily in batch (although they can be run through TSO and SPF), that read SMF files to produce audit trails of ACF2 control file changes, security violation attempts, and logging and trace requests of users or resources.

If an installation is performing investigative work, it might desire additional output (e.g., only selected fields of selected records). ACF2 provides programs that input either the SMF files or the ACF2 control databases and produce user tailored output.

Finally, the ACF2 system includes a recovery program that uses a backup of an ACF2 control file and the SMF files to reconstruct an ACF2 control file if it becomes unusable. An example of a file becoming unusable would be a file residing on a disk pack that is experiencing hardware problems. This recovery is parameter-driven so that, for example, it can be run for select date and time ranges.

MUSASSs (Multiple User Single Address Space Systems) are special applications that require ACF2 interface code to be imbedded in them. IMS and CICS are examples. When they are read into the system, they look like normal jobs and are subject to normal job validation for system and dataset accesses. Subsequently, multiple users sign on and issue transactions. These individual requests should also be intercepted and validated by the ACF2 SVCs, and this is the function of the IMS and CICS interfaces that are supplied with ACF2.

The modifications add a macro, whose name is ACFSVC, within CICS and IMS code. It formats requests and calls the ACF2 SVCs to perform validations based on the actual individual user's request. If the user is authorized, control is passed to the normal CICS or IMS function for completion; otherwise the request is aborted.

ROSCOE is another example of a MUSASS. When it is read into the system, it looks like a normal job and is subject to normal job validation. Subsequently, users sign on, process datasets, and submit jobs. These requests should be intercepted and validated by the ACF2 SVCs, and that is the function of the ROSCOE interface that is supplied with ACF2.

The modifications add the ACFSVC macro to call the ACF2 SVCs to perform Logonid and dataset access validation for users. With dataset accesses, this produces a two level validation. First, the ROSCOE intercepts call the ACF2 SVCs to determine if the user is allowed access to the dataset, then the operating system intercepts call the ACF2 SVCs to determine if the ROSCOE region is allowed access to the dataset.

Summary

This document has attempted to present a conceptual description of the basic components and processing of the ACF2 system. For the sake of brevity and clarity, many details, options, and features have been omitted. That information is explained in the the various ACF2 manuals distributed with the product and is also presented in the ACF2 training classes.