GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

ACF2 MAINFRAME SECURITY

By: Bethany Hinsch

Option 1, Version 1.4b

GSEC

© SANS Institute 2003, Author retains full rights.

ABSTRACT

This document will discuss the specific security features and parameters of Computer Associates' Access Control Facility 2 (ACF2). ACF2 is a mainframe security software utilized to protect the mainframe and it's resources. The document begins by looking at the general area of mainframe security and those security software components utilized to protect mainframes. It continues by focusing solely on the security structure of ACF2, including the listing of common ACF2 records and privileges.

The document then describes the various security parameters and features of the system in the following areas:

- identification and authentication
- access control
- object reuse
- auditing.

It should be noted that some of the ACF2 security parameters listed within this document may be located differently within the ACF2 report obtained, depending on the version of ACF2 that is used. Additionally, this document does not discuss the additional security documentation and/or physical protection required for the ACF2 system.

INTRODUCTION

Mainframe computers support seventy to eighty percent of the world's corporate data.[1] How is it then that mainframe security usually overlooked and/or considered less important? Well, despite the test of time, mainframe computers are still not widely known for security breaches such as, being hacked into or receiving a virus. However, as more tools and software are developed to integrate existing mainframes with more recent distributed systems, the need to protect mainframes and the data they protect grows. Currently, there are three main security products used to protect mainframes:

- Computers Associates' Access Control Facility 2 (ACF2)
- Computer Associates' Top Secret (Top Secret).
- International Business Machine's Resource Access Control Facility (RACF)

This document will solely discuss the process of securing a mainframe server using the ACF2 security system as a means of protection.

ACF2 OVERVIEW

ACF2, also referred to as CA-ACF2, was first released in 1978 by a company named SKK. It was not until 1987 that ACF2 became a product of Computer Associates. ACF2 uses algorithms, called rule sets, to determine if a user is allowed access to a data set or some other resource. A rule set is composed of resource or access rules which are compiled by an authorized user (e.g., system administrator). These rule sets

[1] Korzeniowski, p.2

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

are translated into object records which are stored in the ACF2 Rule or Infostorage database. When a user accesses a specific data set, ACF2 translates that rule set to see if the user has access to that particular data set.

Other control features of ACF2 include special controls over programs, such as Time Sharing Option (TSO) commands. The TSO is a general purpose programming/operating environment which allows multiple users of a host to operate independently. Additionally, ACF2 provides numerous records and reports to assist in security audits and the general administration of the system.

ACF2 RECORDS

ACF2 operates as an extension to the mainframe operating system which is already installed (e.g., OS/390, z/OS). By default, ACF2 users may only access data if granted authorization utilizing a rule by the security administrator or the owner of that data. ACF2 is tailored to individual users and resources by use of the following rules and records:

Rules (records)

- Access Rules: Determines whether access is provided for a certain user or user group to particular data sets.
- Resource Rules: Determines user access to specific resources (e.g., temporary storage, site defined resources, programs).

Records

- Cache Records: Site defined cache facility options.
- Command Propagation Facility (CPF) Records: Site defined CPF options and the CPF network communication configuration.
- Cross-reference Records: ACF2 Mainframe Virtual Security (MVS) validation processing site defined source and resource groups.
- Entry Records: Site defined sources (e.g., terminals) or group of sources which a specific user logonid can access the system from.
- Field Records: Site defined access to records based on fields. The desired ACF2 validation method is specified in an EXPRESSN record and the specified record to use this validation method is specified a RECORD definition record.
- Global System Option (GSO) Record: Specifies the global system configuration. The GSO record will be analyzed, from a security aspect, in more detail later within this document.
- Identity Records: Contains extended user authentication information.
- Loginid Records: Defines users in terms of identification, privileges, access history, violation statistics, and other user information specific to a user loginid.
- NET Records: Specifies distributed database options.
- Profile Records: Contains security-related information about users and resource which can be requested by the system. Profile data information that can be extracted for users includes: WORKATTR, OPERPARM, LANGUAGE, and OMVS.
- Scope Records: Limits authority that a privileged user has over access rules, logonid records, and over ACF2 records.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Shift and Zone Records: Defines periods of times when access is permitted or prevented. Zone records only apply when first accessing the system.

TSO commands, batch utilities, and Interactive System Production Facility (ISPF) panels can be utilized to update each of these components. ACF2 contains three different databases to store these records which include:

- Inforstorage database: Contains resource rules, entry records, field records, cross-reference records, scope records, shift and zone records, global system option records, identity records, and fields records.
- Logonid database: Contains the logonid records for all system users.
- Rule database: Contains all data set access rules.[2]

Additionally, some logonid record fields may grant special privileges/access to system data and resources.

ACF2 PRIVILEGES

Logonids can be granted more than one privilege. The fundamental privileges that may be granted to system users are described as follows:

- ACCOUNT: Allows a user to create, delete, modify, and display logonid records within the limits defined by his or her scope.
- AUDIT: Displays loginid records, infostorage (i.e., an ACF2 defined database) records, and resource and access rules. This privilege allows a user to display ACF2 system controls, but not to modify any of these controls. A user cannot modify any logonid records or access any resources unless he/she is authorized to.
- CONSULT: Displays most fields of loginid records, but only updates nonsecurity-related fields pertaining to TSO. The site at where the system is hosted defines the fields permissible to by modified and displayed by the user.
- LEADER: Displays most logonid records but with increased authority for updating fields within these records as specified by the site.
- SECURITY: Allows access to all resources, data set, and protected programs. A user with this privilege is usually labeled as the security administrator. This privilege does not allow a user to create or delete a loginid, unless the user also has the ACCOUNT privilege.

Other special privileges and actions granted by fields within the logonid record include:

- MAINT: Allows any type of access to a maintenance job resource or data set without logging or rule validation.
- NON-CNCL: Enables full access to any resource and/or data set despite security violations that occur during that attempt. This privilege is not restricted by a scope record.
- READALL: Allows users to read and execute all programs, regardless of specified access rules.

[2] Computer Associates, p.1-3.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- STC: Specifies that a logonid is used for started tasks only. The STC (Started Tasks) field of the GSO record determines the validation of started tasks.

Additional privileges can be specified within the loginid record. All of these privileges should be assigned depending on the users role within the system. The rest of this document will address security parameters that can be specifically controlled by ACF2. Most of these parameters may be displayed by utilizing the SHOW ALL command. These parameters will be discussed in the security areas of identification and authentication, access control, object reuse, and auditing. Although, this document does not address encryption, an organization should use an approved encryption method when transferring sensitive data over the network.

IDENTIFICATION AND AUTHENTICATION

Each user with system access should be granted a logonid and password. ACF2 allows logonids to be from one to eight characters. No source checking is performed for started task logonids during system entry validation.

Passwords authenticate the identity of the logonid and like logonids, ACF2 permits passwords to be from one to eight characters. Passwords may consist of any alphabetic, numeric, or U.S. National character (e.g., @, #). Upon user logon ACF2 builds a user identification string which identifies a user or group of users to reduce the amount of resource or access rules which must be defined.

Besides the use of logonids and passwords, there are many other I&A options which may be set system wide for users. The following settings located under the "OPTIONS IN EFFECT" section within the GSO control options may also be configured:

- JOBCK or JOB CHECK: Denotes that logonids submitting batch jobs are authenticated via the JOB attribute when configured as YES.
- MAXVIO or MAX VIO PER JOB: Indicates the maximum amount of access violation permitted before ACF2 terminates the job session. The default value of this parameter is ten and the maximum value for the parameter is 32767.
- UADS (User Attribute Data Set): Allows ACF2 to validate only the logonid, password, and group supplied at logon. All other logon parameter (e.g., ACCT) are controlled by normal TSO processing. This occurs if UADS is enabled and configured as USE. If this setting is set to BYPASS, then ACF2 controls the all logon parameters and resulting TSO attributes. It is a general best practice not to utilize the UADS option and allow ACF2 to authenticate a user logon utilizing fields within the logonid records.

Other GSO control options which may be configured for I&A are located under the "PASSWORD OPTIONS IN EFFECT" section. These options include:

- LOGON RETRY COUNT: Indicates the maximum number of unsuccessful logon attempts allowed before a session is terminated.
- MAX PSWD ATTEMPTS: Specifies the maximum number of unsuccessful, consecutive password attempts allowed before a logonid is disabled.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- MIN PSWD LENGTH: Denotes the minimum number of characters required for user passwords.
- PSWD ALTER: Allows user to change their passwords if configured to YES.
- PSWD FORCE: Forces users to change their passwords whenever someone other than that user changes his or her specific password if configured to YES.
- PSWD HISTORY: Enforces a maximum password history of four when configured as YES.
- PSWD-LID: Prevents passwords from being equivalent to a user's logonid when configured as YES.
- PSWD-JES: Allows batch job password violations to be counted toward MAX-PSWD ATTEMPTS when configured as ON.
- PSWD NUMERIC: Prevents passwords from being composed of all numeric characters when configured as YES.
- PSWD REQUIRED: Specifies that passwords are required for all logonids (except RESTRICT and STC) when configured as YES.
- PSWD RESERVE WORD: Indicates users are prohibited from constructing new passwords beginning with a reserved word prefix when configured as YES.
- PSWD WARN DAYS: Indicates the amount of days a user is warned before MAXDAYS is enforced.

Many of these password parameters are ignored and/or required to be configured a certain way when local exits are specified for the system. For example, if NEW PSWD VALIDATE which is specified under the "LOCAL EXITS SPECIFIED ON THIS SYSTEM" within the GSO control options is configured as YES, then PSWD NUMERIC should be configured as NO in order to enforce this exit routine. When NEW PASWD VALIDATE is enabled then additional I&A features can be enforced. For example, passwords may be configured to contain alphanumeric characters.

Additional GSO control options which may want to be configured and their location within the GSO control options are:

- LOGON WAIT TIME: Located within the "TSO RELATED DEFAULTS ACTIVE," it denotes the number of seconds before ACF2 aborts logon if the user does not respond.
- NOTIFY: Located within the "OTHER" section of "SYSTEM PARAMETERS IN EFFECT," it indicates that the date and time of the user's last logon is displayed when the user logs onto the system if configured to YES.
- Options listed within "NJE OPTIONS IN EFFECT" if Network Job Entry (NJE) is utilized.

Other parameters which enforce I&A features are located in the specific user logonid records. One of these parameters is MAXDAYS which enforces password aging. It specifies the maximum number of days permitted between password changes before password expiration. If this field is configured as zero, then no limit is defined. Use of either the LIST command or the Super List (ACFRPTSL) report generator will display this option. Logonid records should be reviewed regularly to verify that inactive or unneeded logonids are removed from the system.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ACCESS CONTROL

Besides the many configurable identification and authentication features of ACF2, it provides many access control features as briefly discussed earlier in this document. Privileges, such a those listed earlier (e.g., SECURITY, AUDIT, NON-CNCL), should be restricted to only those users authorized to utilize those privileges. Additionally, several program lists need to be reviewed including:

- MAINTENANCE LOGONIDS/PROGRAMS/LIBRARIES: Identifies the logonids for each user permitted to bypass access rule validation when executing the specified program from a specified library. Logonids specified in these program entries are required to have the NON-CNCL or MAINT privilege.
- RESTRICTED PROGRAM NAMES: Identifies programs with the ability to bypass OS integrity. Execution of these programs is restricted to users with the unscoped SECURITY privilege or users with the NON-CNCL privilege.
- TAPE BYPASS LABEL PROGRAMS/LIBRARIES: Identifies the programs that have the authority to utilize tape bypass label processing (BLP) when executed from a specific library.

Information for each of these programs lists may be displayed within the ACF2 Control options (GSO record) or by utilizing the SHOW PROGRAMS command.

Another option which should be reviewed is the MODE option within the ACF2 control options (GSO record). The MODE option may be configured with the following five settings:

- ABORT: This is the default value for MODE and records all attempted access violations. Access to a data set is denied unless explicitly defined.
- LOG: This value logs all data set violations but still allows data set access to continue.
- RULE: Deemed an interim mode, this value allows actions to be performed if an existing rule set does not permit a user's request to a data set.
- QUIET: Disables ACF2 data set access rule validation. All access attempts are permitted and no access violations are logged.
- WARN: Permits all access attempts and logs any access violation that occurs. If an access violation occurs, the user is notified by a system generated error.

For security purposes, MODE should be configured to ABORT to disallow data set access unless explicitly defined and to log all access violations.

Additional access control options may be displayed within the appropriate section of the GSO control options. These options include:

- DECOMP AUTHORITY: Located under the "RULES/DIRECTORY RESIDENCY OPTIONS" section, this setting identifies the type of privilege, users need to have in order to display access and resource rules, despite scope restrictions.
- DSNAME PROTECTED VOLUMES: Located under the "RULES/DIRECTORY RESIDENCY OPTIONS" section, this section should be reviewed to ensure that

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Direct Access Storage Device (DASD) data sets and volumes are protected by RESVOLS. The RESVOLS record defines storage volumes and DASD to provide protection at the data set name level.

- INFO LIST AUTH: Located under the "RULES/DIRECTORY RESIDENCY OPTIONS" section, this setting identifies the type of privilege, users need to have in order to display and list records stored in the Inforstorage database.
- NOSORT: Located under the "OPTIONS IN EFFECT" section, this setting indicates that access rule sets are sorted in order of the most specific rules to the most general rules when configured as NO.
- TAPE DSN: Located under the "OPTIONS IN EFFECT" section, this setting indicates that tape data set protection is enforced before granting access when configured as YES.
- QUICK LOGON: Located under the "TSO RELATED DEFAULTS ACTIVE" section, this setting indicates that users are forbidden to enter their individual password and logonid on the same line when configured as NO.
- UID: Located under the "RULES/DIRECTORY RESIDENCY OPTIONS" section, this setting identifies the type of privilege, users need to have in order to alter the UID string. The UID string is composted of concatenated fields which control each user's UID record definition.
- VOLSER PROTECTED VOLUMES: Located under the "RULES/DIRECTORY RESIDENCY OPTIONS" section, this section should be reviewed to ensure tape volumes and DASD volumes are protected by SECVOLS. The SECVOLS record defines the tape, DASD, and storage volumes to provide volume level protection.

GSO control options provide many access control parameters which need to be reviewed. Logonid record fields which contain information about individual users should also be reviewed and restricted for the following privileges:

- ALLCMDS (NOALLCOMDS): Indicates the ability to bypass ACF2 restricted command lists.
- REFRESH (NOREFRESH): Indicates that users can issue the REFRESH command. The REFRESH command allows users to modify/update the records within the Inforstorage database.
- RULEVLD (NORULEVLD): Indicates that an access rule authorizes user data set access for data owners and users with the SECURITY privilege.
- TAPE-BLP (NOTAPE-BLP): Indicates that a user can use BLP when accessing data sets.

These privileges should be granted only to authorized users. Additionally, the Access Rules (report) should be reviewed for all distribution libraries (which contain load modules for ACF2 [e.g., ISPF panels]), sensitive data sets (e.g., critical SYS1 data sets [with the exception of SYS1.MAN]), and ACF2 protected databases (e.g., SYS1.ACF.* data sets and libraries disallow the ALLOCATE and WRITE privileges unless needed for emergencies).

OBJECT REUSE

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In addition to I&A and access control features, ACF2 provides a configurable capability to remove data sets and volumes from the system. The Automatic Erase (AUTOERAS) feature of ACF2 specifies whether ACF2 is utilized to physically remove data sets and volumes when a user deletes them. This setting may be reviewed in the "OPTIONS IN EFFECT" section of the GSO control options.

AUDITING

The last ACF2 security area addressed by this document is the configurable capability of ACF2 to perform auditing and record this information in logs. As discussed previously, the SHOW PROGRAMS command, will display the list of programs running on the system. This list should include "LOGGED PROGRAMS" which should log programs and libraries, including:

- MAINTENANCE LOGONIDS/PROGRAMS/LIBRARIES
- RESTRICTED PROGRAM NAMES
- TAPE BYPASS LABEL PROGRAMS/LIBRARIES.

Additionally, the following settings located within the GSO control options may also be configured to generate and/or protect audit information:

- ACF2 COMMON: Located under the "SYSTEM PARAMETERS IN EFFECT" section and "SMF RECORD NUMBERS" subsection, this setting identifies the SMF log key record number for ACF2 functions.
- TAPE BLP: Located under the "OPTIONS IN EFFECT" section, this setting indicates that an audit log is generated when users are program bypass tape label processing when configures as LOG.
- STC OPTION: Located under the "OPTIONS IN EFFECT" section, this setting indicates that a system task must be authenticated by ACF2 before being granted access to a data set when configured as ON.

Audit logs should be reviewed by an organization on a periodic basis and information recorded within the audit logs should be sufficient to adequately audit the system. The amount of information that is recorded and/or needed is dependent upon the system, the data stored within the system, and the organization controlling the system.

CONCLUSION

Mainframe computers support seventy to eighty percent of the world's corporate data. Therefore, why not utilize security software to protect them? As shown, there is a vast array of methods and means to protect mainframe computer systems. Utilizing them will protect many systems from Denial of Service (DoS) attacks and other security breaches.

In dealing with security for mainframes it helps if the system administrator enables and utilizes as many different options as needed to protect the data and logonids stored within the system. These security settings, data sets, etc. should be enforced by the organization's security policy. In addition to the security of the computer software, the physical security of the hardware that the software resides on should be secured.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

REFERENCES

Abramson, Christopher. "A Return to Legacy Security." SANS. 27 July 2001. http://www.sans.org/rr/main/legacy.php (15 January 2003).

Barker, Chad. "Mainframe Security featuring CA-Top Secret." SANS. 20 February 2002. http://www.sans.org/rr/main/top_secret.php (15 January 2003)

Computer Associates. CA-ACF2 6.1 MVS Administrator Guide. Computer Associates International, Inc. 1994.

Computer Associates. CA-ACF2 6.1 MVS Auditor Guide. Computer Associates International, Inc. 1993.

Computer Associates. CA-ACF 6.4 Release Guide. Computer Associates International, Inc. 1993. http://support.ca.com/techbases/acf2/ACF64OR.pdf (24 March 2003)

Computer Associates. eTrust CA-ACF2 Security for z/OS and OS/390. October 2002. http://support.ca.com/CA-ACF2supp.html. (23 March 2003).

LeClerc, Rey. "ACF2/VM Review." http://www.auditnet.org/docs/acf2vm.txt (1 March 2003).

Korzeniowski, Paul. "Audit and Assessment." Information Security Magazine. August 2000. http://www.infosecuritymag.com/articles/august00/columns6.shtml (10 March 2003)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.