MANEWS Issue Number 25

the Mainframe Audit News

This newsletter tells you stuff you need to know to audit IBM mainframe computers running with z/OS and the MVS operating system. This issue we explore the new releases of z/OS, MVS, and RACF, as well as some critical, but often ignored aspects of mainframe security.

Table of Contents

1. New Features with New: z/OS and RACF 2.2
2. USS: Often Ignored in the Audit, Essential to Security
3. TCP/IP: Often Ignored in the Audit, Essential to Security
4. Free Webinar: "How to Go About Setting Mainframe Security Options" November 17 and 18

Appendices Seminar Information and Miscellanea
Subscribe / Unsubscribe

1) New Features with New: z/OS and RACF 2.2 (ACF2 andTopSecret R16 should be available this month. We hope to have details next issue.)

IBM has just delivered z/OS version 2.2, along with RACF 2.2. Here are some of new features you'll see:

For z/OS 2.2

- Digital signing of SMF log records to ensure that they haven't been altered and that they came from the correct source (non-repudiation). The system uses message digests to ensure this, similar to the message signing used with copies of programs, and with SSL. (Note that this feature may add to CPU usage,

but may also be subject to regulatory requirements for records retention.)

- Faster encryption, with more of the standard algorithms supported. (This may reduce CPU usage.)
- New SMF record type to monitor dynamic changes to the list of APF authorized datasets. This means when someone adds new APF authorized datasets dynamically (by means of the SET PROG or SETPROG operator commands, or by means of the CSFAPF programming service), the system can to write new SMF Type 90 subtype 37 records to record the event.
- Improved console security
- Additional checking in the security software for operator commands, using the OPERCMDS resource class
- Enhanced PKI (Public Key Infrastructure) support for managing digital certificates
- Enhanced Kerberos support
- Additonal Healthchecks

Note: The previous releases of z/OS are z/OS 1.13 and z/OS 2.1. The end of support for z/OS 1.13 is September 30, 2016. You can monitor end of support dates for IBM software at http://www.ibm.com/software/support/lifecycle/index_z.html

For RACF 2.2

- A new user attribute named ROAUDITOR (for Read Only Auditor). This is similar to the AUDITOR attribute, which lets you list any RACF rule or profile, and also lets you issue SETR LIST and execute DSMON. However ROAUDITOR does not let you set logging options for SMF. (Neither of these gives you access to data, just the ability to read the RACF rules and options.)

- A change to the ADDUSER command so that if you don't specify a password on the command, it defaults to no password. This is an improvement, since the earlier default could lead to easily guessable passwords.

- Stronger encryption for passwords and password phrases in the user records in the RACF database using an algorithm named **KDFAES** (Key Derivation Function with AES)

- The ability to allow additional special characters in passwords.

- Removal of the need for the ICHDEX01 password exit

- The ability to have userids defined with password phrases, but not with passwords. (This strengthens security. Any userid with a password will fall to a password cracker program faster than the same userid without a password.)

- Enhancements to RRSF (RACF Remote Sharing Facility), PKI (Public Key Infrastructure), and RACDCERT (for digital certificates)

- A new resource class for USS named **FSEXEC**, to control Execute authority within a file system

- A new UNIXPRIV rule named **SUPERUSER.FILESYS.DIRSRCH** to permit users to search directories without letting them change the data in files

- Additional health checks covering controls over ICSF, USS Services, and RRSF) resources, as well as use of password options and encryption methods.

What This All Means to Your Audit

This calls for no major change in your audit program. If you're auditing a RACF shop, your userid might have the ROAUDITOR attribute instead of AUDITOR. You might see what plans are underway to take advantage of the new features. You will want to check, as always, that the system software is on a currently supported release. If your audit program doesn't address Healthchecks, this would be a good opportunity to do so. Perhaps more important than staying on top of the new features is ensuring that USS and TCP/IP are adequately addressed in your audit program, as outlined in the next sections.

2) USS: Often Ignored in the Audit, Essential to Security

USS (UNIX System Services, formerly called OMVS) is standard UNIX on the mainframe, under the control of your security software (RACF, ACF2, or TopSecret). Mainframe security audits often ignore it completely. This is a mistake for several reasons:

- Configuration files for TCP/IP and related programs such as FTP are often USS files. USS file security is essential for change control over these files, and by extension to network security.
- USS contains callable services (similar to APIs) that allow users to assume the identity (the RACF, ACF2, or TopSecret identity) of other users
- Production applications are starting to be implemented in, or ported to, USS
- USS security is easier to maintain if it is implemented properly from the beginning. But there are several options which relax the security architecture. These options can seem convenient to set, but weaken the overall security architecture.

Here's a little background on USS security, and how it relates to other UNIX security you may be familiar with.

- Like other UNIXes, USS identifies users with numbers called UIDs, and identifies groups of users with numbers called GIDs. In USS these UIDs and GIDs are stored with the security software user records, providing centralized security administration for the mainframe. This also eliminates the /etc/passwd file, which is a source of many security exposures in other versions of UNIX.

- Access control for USS files is based on the same RWX (ReadWriteeXecute) specification as other UNIXes. In USS the evaluation of whether a given user can access a given file is by default controlled by the security software. This allows RACF, ACF2, or TopSecret to provide greater granularity for delegation of authority. That is, you can give a user power somewhere between being superuser and being no one.

- ACF2 and TopSecret both have options so replace the standard RWX file access control with rules in the security software. You can see these in the SHOW ALL and TSS MODIFY(STATUS) command outputs.

To start to address USS security in your audit:

- Inquire what applications are using USS.
- Inquire whether TCP/IP (which relies on USS for security) is in use on the mainframe, and for what applications
- Inquire what risk assessments have been performed for USS security and the applications which use it.
- Inquire who is responsible for USS security.
- Learn of any baseline documents detailing how options are to be set.
- Inquire what use is being made of USS callable services which can permit USS programs to bypass the rest of mainframe security. (Techniques include several ways of making USS programs be APF-authorized and the ability to assume the identity of other users.)
- Get copies of the USS configuration file, which is almost always a member of the MVS parmlibs with a name like BPXPRM...
- From the security software, find out which users have root privilege.
- From the security software, get copies of rules in the UNIXPRIV resource class, as well as FACILITY class rules whose names begin BPX....
- From the security software options reports (SETR LIST in RACF; SHOW ALL in ACF2; TSS MODIFY(STATUS) in TopSecret), determine what USS relevant options are set. These often have names beginning OMVS, BPX, or HFS.
- Assign audit resources appropriately.

3) TCP/IP: Often Ignored in the Audit, Essential to Security

Mainframes with z/OS have standard TCP/IP, built on top of the USS UNIX software. This is standard TCP/IP, based on IP addresses and port numbers. It may be connected, directly or indirectly, to the Internet. It supports all the standard daemons such as FTP and telnet. It also allows programs such as CICS, DB2, and MQ to connect to Windows and UNIX computers in your organization. The TN3270 software lets users sign on to the mainframe over TCP/IP, and often over the Internet.

It is very common for a data center to have Windows and UNIX computers facing the Internet but also connected to the mainframe. The connection between these distributed computers and the mainframe is a common source of security exposures. This is often the result of no one being responsible for securing the connection properly. There are outstanding, free tools on the mainframe to secure its TCP/IP connections. One of the best of these is named Policy Agent, or PAGENT for short. It provides firewall functions, including: encryption, blocking of ports, intrusion detection, packet filtering, IPSEC, and virtual private networks (VPN). It is very rare for a mainframe data center not to be using mainframe TCP/IP.

To start to address mainframe TCP/IP in your audit:

- Ask who is responsible for mainframe TCP/IP security.
- Ask what applications are using TCP/IP on the mainframe.
- Even if the answer is “none”, ask to see the output of the TSO command NETSTAT. This will tell you all the programs and all the connections using TCP/IP. If this list is empty, then perhaps TCP/IP is not being used on the mainframe. More likely, the list will include programs such as FTP, TN3270 (remote logon), CICS, DB2, MQ, and others.

- Note whether Policy Agent is in use (appears as PAGENT in the NETSTAT output).
- Note in the security software whether the SERVAUTH resource class is active, and what rules exist. This lets RACF, ACF2, and TopSecret help to secure TCP/IP.
- Inquire what risk assessments have been performed. Learn of any baseline documents detailing how options are to be set.
- Inquire what encryption is used with TCP/IP, for passwords, and for other sensitive information
- Assign further audit resources as appropriate.

4) Free Webinar on Setting Security Software Options

Stu Henderson will once again present on the z Channel Tuesday and Thursday, November 17 & 19, 2015 - 2 pm EST (11 am PST) **"*How to Go About Setting Mainframe Security Options*"** shows you how to go about about deciding how to set security options in RACF, ACF2, or TopSecret**.** This presentation won't attempt to tell you how every setting should be set; it will show you how to think about them for yourself in ways that make life easier and security more reliable. For info, or to register for this free session: http://www.newera-info.com/Stu_Henderson.html

(You can also see there handouts from earlier webinars, including "***Top 12 Mainframe Security Exposures and Lessons From A Real Mainframe Break-In***", "***JUST FOR CIOs - Managing Mainframe InfoSec More Effectively***" and "***How to Secure Mainframe TCP/IP***")

Appendices: Seminar Information and Miscellanea

Appendix A) >>>>Seminar Information

Henderson Group seminars are available for in-house as well as public sessions.

The Henderson Group offers these "How to Audit..." courses :

- How to Audit **z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (May 10-13, 2016 in Raleigh, NC and Sept. 19-22, 2016, location to be determined)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (November 15-17, 2016 in Bethesda, MD), a logical follow-on to the previous course
- How to Audit **UNIX and Windows Security** (October 24-27, 2016 in Bethesda, MD)

To learn more about them, please go to

http://www.stuhenderson.com/XAUDTTXT.HTM

Appendix B) >>>>This Issue's Proverb of the Day

"*No matter where you go, there you are. That's your starting point.*"

Appendix C) >>>>Useful Information

Here are more useful information sources to help you audit more effectively:

1. New Era offers free webinars by top speakers, and free books to help you audit mainframes better. You can see the seminar schedule and get handouts from previous sessions at
   http://www.newera-info.com/zwebs.html
   To get the free books: www.newera-info.com/AE.html

   Book topics include:

   - AE2 - z/Auditing Essentials - Volume 2 - The Taming of SETROPTS
   - AE1 - z/Auditing Essentials - Volume 1 - zEnterprise Hardware - An Introduction for Auditors
   - CICS Essentials - Auditing CICS - A Beginner's Guide
   - What's New in z/OS V2R2

2. The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes
   https://web.nvd.nist.gov/view/ncp/repository

3. Useful guidelines for knowing that your InfoSec is comprehensive (Note especially Publication 800-53):
   http://csrc.nist.gov/publications/PubsSPs.html#800-53

An additional source of free, practical information on mainframe security and auditing, from a variety of sources:
http://www.stuhenderson.com/XINFOTXT.HTM

Appendix D) >>>>About the Mainframe Audit News; Subscribe/Unsubscribe

The MA News is a free, email, newsletter for auditors who need (or suspect that they will need) to be auditing IBM mainframe systems (primarily **MVS**, **z/OS**, and the system software associated with them). This software includes: **CICS**, **DB2**, **JES**, **VTAM**, **MQSeries**, **TSO**, **USS** (UNIX System Services), **TCP/IP**, and others.

It also includes the **httpd daemon** software which connects a mainframe to the Internet. (Note, we expand each of these acronyms and explain how the software works in past and future issues.) The MA News is for auditors who are new to IBM mainframes, and also for experienced MVS auditors who want to keep up to date with the latest developments. We will not make the list of subscribers available to anyone else for any reason.

To Subscribe or Unsubscribe Click on
http://www.stuhenderson.com/subscribe.html .

To see Back Issues: www.stuhenderson.com/Newsletters-Archive.html

Feel free to contact us at (301) 229-7187 or stu@stuhenderson.com.