MANEWS Issue Number 19

the Mainframe Audit News

This newsletter tells you stuff you need to know to audit IBM mainframe computers runinng with z/OS and the MVS operating system. Please see Section 7 for more information. This issue we show you several new information sources, and talk about different ways to form your audit report..

Table of Contents

1) How to Learn Mainframe TCP/IP Connections

Now that mainframes support standard UNIX (USS) and standard TCP/IP, they are starting to be used as Internet platforms. In addition to the standard daemons like FTP, telnet, and httpd, mainframe TCP/IP also supports Internet connections for CICS, DB2, MQ Series, and other mainframe software.

As you plan your upcoming audits, you might wonder whether you should be including mainframe TCP/IP in your plans. IT staff may tell you that they are doing nothing with mainframe TCP/IP. To confirm that they are correct, you can issue the TSO command NETSTAT.

This command (like netstat in Windows and UNIX) will list TCP/IP connections, including the to and from sockets (IP addresses and ports), and the programs that are using them. Now you will be in a position to decide to exclude mainframe TCP/IP from your upcoming audit plans, or not.

==========
==========

2) Another Way to Get Supervisor State

To simplify mainframe audits, we break mainframe security into two components. The first is the security software (RACF, ACF2, or TopSecret) which handles userids, passwords, dataset protection, and resource protection.

The other component is the security of the MVS operating system itself, which relies on hardware controls such as Supervisor State. The MVS operating system uses the hardware controls to build a virtual cage around each executing program, preventing one program from interfering with any other program.

However, any program which is given Supervisor State can break out of its virtual cage, and then bypass all the security on the system (including the security software). You may be familiar with some of the standard methods for granting a program Supervisor State. These include APF (Authorized Program Facility), user supervisor calls, and others.

One additional way to grant obtain Supervisor State is often missed in mainframe security audits. This way is called **CSVAPF**. CSVAPF is a request by a program to make an existing dataset be APF-authorized. Any program which is allowed to issue CSVAPF specifying certain options can mark a program library as APF-authorized. A programmer who is permitted to do this could use CSVAPF to obtain Supervisor State,and then to bypass all the security on the system.

(The specific technique would be to create a program library (that is a dataset containing executable programs). The programmer would then write a program which issues a MODESET (request for Supervisor State) and then move that program into the new program library, marking the program APF-authorized. The programmer would then execute yet another program which would issue a CSVAPF to mark that program library APF-authorized. The result would then be that when the new progarm in the program library executes, it would obtain Supervisor State and be able to bypass all the security on the system.

So what controls are there to limit who can issue a CSVAPF? The first part of the answer is that you need to have Supervisor State already, in order to issue CSVAPF. The second part of the answer is that there is an exception to the first part: if a user has UPDATE permission in the security software to a rule in the FACILITY resource class named CSVAPF.xxx, then the user doesn't need Supervisor State to issue the CSVAPF.

(Note that the xxx in the name of the rule can be either the dsname of the dataset to be APF-authorized or a wildcard which would match any dsname. Note also that the FACILITY resource class is called in TopSecret the IBMFAC resource class. For ACF2, the FACILITY resource class usually corresponds to type FAC.

What To Do In the Audit?

Check the security software rules to see if FACILITY class rules exist with names beginning **CSVAPF**. . If so, see who has UPDATE access to those rules, since UPDATE access to these rules gives a programmer the ability to bypass all the security on the system. If there are no such rules, then there is no risk here to address. If there are such rules, evaluate the approval process which resulted in users having UPDATE access to them. Determine from the rules whether checking against them is logged, and whether a responsible, independent manager reviews the resulting report.

==========
==========

3) TwoTones of Voice for an Audit Report

One of the most common complaints about IS audit reports is that they appear to criticize the IT staff for not doing what some checklist says they should be doing. Whether or not IT staff agrees with the checklists, the reports sometimes appear directed towards criticizing people (known as ad hominem attacks).

A different approach to writing audit reports would direct attention to the tools available to IT management. Using extreme examples to make the point, rather than stating "IT management has failed to prevent unsafe privileged programs from

being added to the system", the report could state something like "IT management does not have the tools available to them to ensure that no privileged program is added to the system without formal approval, testing, and documentation. Management has indicated that they would like to have and to implement such tools, which might include change management software and more restrictive rules in the security software."

Yes, these are extreme, perhaps ridiculously extreme, examples. But they illustrate the difference in tone of voice. As you review the drafts of your audit reports, you might ask yourself two questions: "If I were the auditee, would I feel unjustly attacked?" And "If I were asked to implement the recommendations I'm making, would I be comfortable that they are doable?"

==========
==========

4) Standards to Audit Against

We sometimes wonder what standard we should be auditing against when auditing mainframe security. Here are some possible sources of standards for mainframe audits:

4a) IBM provides a list of recommended protection for system datasets. While this is available in a RACF manual, what it says may easily be applied to ACF2 and TopSecret. The manual is "Security Server RACF Security Administrators Guide", and you can download it as a pdf for free from: http://publibz.boulder.ibm.com/epubs/pdf/ichza7c0.pdf . Look in Appendix D "Security for System Datasets". Note that in RACF the word UACC just means "default access allowed".

4b) IBM also provides us with a list of IBM-supplied entries in the Program Properties Table. (This MVS table is one technique for assigning privileges such as privileged protect keys to programs. Two of these privileges are important for secuirty. One of them is a privileged called protect key. Any protect key from 0 to 7 is considered privileged in that it makes the program able to bypass all the security on the system. The other privilege is named Bypass Password Protection or BP. A program

with the BP privilege bypasses RACF or TopSecret protection for datasets. That is, when it opens a dataset, the open function does not call RACF or TopSecret, letting the program open any dataset it wishes. This privilege should only be given to programs known to be "safe". One way of knowing that a progarm is safe is to know that it is covered by IBM's Integrity Statement for MVS, which we have described in earlier issues. The IBM-supplied entries may be considered to be covered by this.
You can find the list of IBM-supplied entries in *"MVS Initialization and Tuning Reference*" which you can download for free in pdf format from:

http://publibz.boulder.ibm.com/epubs/pdf/iea2e2c2.pdf

Look for members named SCHEDXX in the table of contents.

4c) IBM provides another list: the list of started tasks which should be marked TRUSTED in RACF. (ACF2 installations might give these same started tasks a userid with the NON-CNCL attribute.. TopSecret installations might give them a userid with the NODSNCHK attribute.) This list is found in the same IBM manual "*MVS Initialization and Tuning Reference*". Check the Table of Contents for "Assigning the RACF Trusted Attribute".

4d) One possible source for standards is the STIGs (Security Technical Information Guide) from the US government. These provide basic lists of things to check when conducting a mainframe audit. You can download the most recent STIGs for RACF, ACF2, and TopSecret from:

http://iase.disa.mil/stigs/os/mainframe/z_os.html

Please note that the G in STIG stands for Guidance, not for Absolute Standard. Not all mainframe data centers accept the STIGs as a standard. However, they can provide you with a useful checklist of things to consider, a checklist which you of course will apply with careful thought and a grain of salt.

What This Means for Your Audit:

Substantive tests of detail in an audit might be described as "comparing what's there to what's supposed to be there". For each of the standards listed above, you can compare what is actually on the system to what the standard says SHOULD be on the system. When you find discrepancies, you do not automatically have an audit finding, of course. You still need to identify the risk, if any.

To see who can write to system datasets, list the dataset rules that match the names of the datasets. RACF installations can use the **LISTDSD** command. ACF2 installations can use **SET RULE** followed by **LIST LIKE(...)**. TopSecret installation can use the **TSS WHOHAS** command..

To see a list of what is currently in the Program Properties Table, for RACF installations, see the **DSMON** report. TopSecret installations can use the **TSSAUDIT** program. You can also learn what is in the Program Properties Table by browsing the parmlib members named **SCHEDxx**, or by running a progarm such as **CA Auditor** (formerly **CA Examine**).

To see a list of the current started tasks, RACF installations can again look at the **DSMON** report. TopSecret installations can issue TSS LIST(STC). ACF2 installations can issue **LIST IF(STC)**.

A starting point for you audit would be to compare what is in these standards against what the installation actually has in place. For entries in the Program Properites Table, and for TRUSTED started tasks that are not recommended by IBM, you would inquire why they are there, what security analysis concluded that they were safe, and whether they are documented as part of a formal change control process.

For any entires not recommended by IBM or contrary to what is in the STIGs, and not the result of an effective change management program, you still need to answer the "so what?" question. This should be easy to do if you are talking about a program that can bypass all security on the system, and which has not been covered by formal approval, security analysis, testing, and change control. For IT governance, you might want to investigate what in the organization led to this state of affairs.

==========
==========

5) New Release Cycle for z/OS

IBM has announced a major change in the frequency of new releases (versions) of z/OS (which include MVS and most of its related software). Until recently IBM gave us a new release of z/OS twice a year. The new release cycle will be once every two years.

This should reduce costs, and also reduce the effort and problems associated with testing and implementing a new release.

This will also reduce, but not eliminate, the need for system programmers to be able to update system datasets without going through a formal change control process. (When going to a new release, whoever is upgrading z/OS will need to update almost all or almost all the system datasets.)

==========
==========

6. Learn How to Improve IS Audit Support of Financial Audits

Stu Henderson is conducting a study of what works and what doesn't work for integration of IS audits and financial. If you would like to take part in a ten to fifteen minute phone interview to share your thoughts and experiences, contact him at stu@stuhenderson.com. Indicate best times for him to call you, and the best phone number. Your name and organization will not appear in the final report unless you authorize it in writing. All participants will received a copy of the final report, which will have recommendations on how to improve this integration..

==========
==========

7) Seminar Information and Miscellanea

7A) >>>>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** (November 12-15, 2012 in Clearwater, FL and May 7-10, 2013 at a location to be determined)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (April 8-10, 2013 in Bethesda, MD), a logical follow-on to the previous course
- How to Audit **TC/IP Security** (May 29, 2013 in Bethesda, MD) **(NEW)**
- How to Audit **UNIX and Windows Security** (September 9-12, 2013 in Bethesda, MD) **(NEW)**

To learn more about them, please go to

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

7B >>>>This Issue's Proverb of the Day

"*When learning something new, we move in stages from Awareness to Awkwardness, to Application to Assimilation to Art*"

7C) >>>>Useful Information

Here's a source of free, practical information on mainframe security and auditing, from a variety of sources. Topics include:

- Glossary of Mainframe Terms
- How to Get z/OS Basic Skills and IBM z/OS Manuals in pdf Format
- Integrity Statements from CA Technologies and IBM
- z/OS Configuration Info: Documents, Audit Guides from NewEra
- Back Issues of z/Journal Magazine and Mainframe Executive Magazine
- IBM Presentation Handouts on Security and RACF from SHARE and GSE
- Free Articles on Mainframe Security and Auditing

Here's the link: http://www.stuhenderson.com/XINFOTXT.HTM

7D) >>>>About the Mainframe Audit News; How to 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 meant for auditors who are new to IBM mainframes, as well as for experienced MVS auditors who want to keep up to date with the latest developments from IBM. We will not make the list of subscribers available to anyone else for any reason.

To Subscribe, Unsubscribe, or Request Back Issues

Send an email to: **stu@stuhenderson.com** with the subject field set to: **MA News** and in the body of the email: SUBSCRIBE or UNSUBSCRIBE or BACK ISSUES: 1, 2