MANEWS Issue Number 21

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. This issue we show you how to plan the data gathering for your audit.

Table of Contents

1) Planning Data Gathering for a Mainframe Security Audit

Getting the data you need at the beginning of an audit may be one of the most important things you can do to make the audit successful. Knowing what to ask for before the audit starts is key to getting it before you need it. You'll learn below how to plan what data to ask for. In future issues we will show you how to interpret some of it, and how to make use of it in your audit program. **This issue addresses only planning for your data gathering**.

To decide what to ask for, consider that mainframe (z/OS and MVS) security consists of two major parts: the security software and the MVS operating system security. You will likely want to limit your scope to one or the other.

The security software is always one of these Big Three:

- **RACF** (IBM's Resource Access Control Facility)
- **CA-ACF2** (CA Technology's ACF2) or
- **CA-TopSecret** (CA Technology's TopSecret, often called just TSS)

The security software handles identification and validation of users (often by means of a userid and password). It also handles access control, such as "Can this user open this dataset for update?" or "Can this user execute this CICS online transaction?".

Each of these Big Three has a set of reports describing basic option settings, such as minimum password length and whether tape datasets are protected. Each of these Big Three also has dataset rules which describe who can read and write specified datasets. (A "dataset" means the same as a "file".)

Each of the Big Three has resource rules which describe who can access resources, such as online transactions, printouts, operator commands, or database tables. The definition of "resource" is "anything other than a dataset that you want to protect". There are literally hundreds of types of resource. Each resource type, sometimes called a resource class, has a unique name, such as **TERMINAL** for terminal resources or **OPERCMDS** for operator commands. All of the resource rules describing, for example, operator commands (and who can execute each one) are said to be "in the OPERCMDS resource class".

So as you plan your audit, decide whether to include the security software in the scope, and whether to include the MVS security in the scope**. If your audit includes the security software**, then learn which of the Big Three is involved and request copies of the reports and rules appropriate to it. Please see the appropriate section of this newsletter below to learn what to ask for.

If you are planning an applications audit, then learn the names of the datasets it uses (based on the data center's naming standards). For example, the standard might specify that all production datasets for the Payroll application have names beginning **PROD.PAYROLL** . Learn what resources the application uses, such as online transactions and database tables, and their names. Again the data center's naming standard might specify that all online transactions for the Payroll application have names beginning **PR**. Then request the dataset rules and resource rules from the security software for that application.

If you are planning an MVS security audit, you need to understand what a privileged program is. IBM has designed the MVS operating system to provide a solid foundation for the security provided by the Big Three. To do this, MVS uses certain hardware controls to build a "virtual cage" around each program that is running. This cage prevents each program from interfering with any of the other programs running in the computer at the same time. IBM is so certain that this architecture provides reliable security that they provide us written assurance in the form of IBM's *Integrity Statement for MVS*.

Each MVS installation will have hundreds of programs added to it which have privileges that permit them to "break out of their cages", and to bypass all security on the system. To have effective security requires controls to know that these privileged programs don't introduce security exposures. Your job as an auditor is not to evaluate the security of these programs. Rather, it is to evaluate the controls management has for them to know that the privileged programs are safe, can't be modified improperly, and are all approved. To do this you will start by identifying the datasets where these programs are stored, and where they are specified.

Please see the section below describing what data to ask for.

USS and/or TCP/IP Audit

When you install the MVS operating system software, you also get for free both USS and TCP/IP. **USS** (UNIX System Services) is a standard version of UNIX that can be the most scalable, reliable, and secure UNIX commonly available, if it is configured properly..

TCP/IP (Transmission Control Protocol / Internet Protocol) is a standard version of TCP/IP, built on top of USS. It can be the most scalable, reliable, and secure TCP/IP commonly available, if it is configured properly.

Both USS and TCP/IP should be addressed as separate audits. If you are doing a mainframe security audit, you should explicitly exclude them from your scope until you are ready to audit them. Otherwise, you run the risk of people assuming that they are inlcuded in your scope. We will address USS and TCP/IP audit data gathering in a future issue.

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

2) What Data to Gather for a RACF Audit

If you have a userid on the system and know how to get reports from RACF, you can get these yourself. If not, request the RACF administrator to get them for you.

- **SETR LIST** (lists the basic options for RACF; for an explanation of how to interpret this, please see http://www.stuhenderson.com/XSETRTXT.HTM)
- **DSMON** (lists further options, including password rules, exits, and more. Consists of 11 sub-reports. You may want to skip the Group Tree Report which can be very large, and which is used only for delegation of authority. For an explanation of how to interpret the DSMON output, please see http://www.stuhenderson.com/XDSMNTXT.HTM)
- Sample of dataset and resource rules (to show you who is permitted what accesses)
- Written approvals (used as a standard against which to evaluate the rules)
- Baseline documents (descriptions of how basic options are to be set, used as a standard against which to evaluate basic options)
- Security policy (used to clarify who has what responsibility and authority)
- Procedures for security administration

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

3) What Data to Gather for a CA-ACF2 Audit

If you have a userid on the system and know how to get reports from ACF2, you can get these yourself. If not, request the ACF2 administrator to get them for you.

- **SHOW ALL** output (to learn how the basic options are set)
- Sample of dataset and resource rules (to show you who is permitted what accesses)
- Written approvals (used as a standard against which to evaluate the rules)
- Baseline documents (descriptions of how basic options are to be set, used as a standard against which to evaluate basic options)
- Security policy (used to clarify who has what responsibility and authority)
- Procedures for security administration

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

4) What Data to Gather for a CA-TopSecret (TSS) Audit

If you have a userid on the system and know how to get reports from TSS, you can get these yourself. If not, request the TSS administrator to get them for you.

- **TSS MODIFY(STATUS))** output (to learn how the basic options are set)
- Copy of control file which is where the TSS administrator sets the options, including more options than you will see from TSS MODIFY(STATUS)).

- Output of the following TopSecret Commands:

  TSS LIST(ALL) to list the ALL record, which specifies datasets and resources to which all users are granted access

  TSS LIST(STC) to see ACIDs assigned to started tasks

  TSS LIST(RDT) to see the resource definition table

  TSS LIST(AUDIT) to see the Audit Record which specifies datasets and resources whose accesses are always logged. (Violations are always logged.)

  TSS MODIFY(FAC(ALL)) to learn facilities (paths into the system)

- Output of **TSSAUDIT** to see which userids have which privileges
- Sample of dataset and resource rules (to show you who is permitted what accesses)
- Written approvals (used as a standard against which to evaluate the rules)
- Baseline documents (descriptions of how basic options are to be set, used as a standard against which to evaluate basic options)
- Security policy (used to clarify who has what responsibility and authority)
- Procedures for security administration

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

5) What Data to Gather for an MVS Security Audit

The privileged programs in MVS are stored in certain system datasets, often called “key datasets”. The names of these key system datasets are specified in other datasets called “parmlibs” (Originally there was just one parmlib, always named SYS1.PARMLIB, but now there may be several others in use as well.)

To learn the names of the parmlibs, request the output of this operator command: **DISPLAY PARMLIB**. The result might list names like this:

MYORG.ALL.PARMLIB
MYORG.SYSA.PARMLIB
SYS1.PARMLIB

Whatever the names are, request copies of all of them. These datasets consist of several “mini-datasets” called members. Request copies of all the members of all the parmlibs. Make sure you receive the contents of all the members, not just a list of the member names.

Once you have copies of the parmlibs, you can read them to learn the names of the datasets containing privileged programs. You will then want to request the dataset rules from the security software for these datasets. The dataset rules will tell you who can write to the key datasets and whether updates to the key datasets are logged. Please note that this issue we do not cover how to read the parmlib members. We will address this in a future issue.

To complete your MVS audit data gathering, ask for the names of the following datasets, and the security software rules which protect them:

– the proclibs, where control statements for batch jobs and started tasks are stored
– the page datasets, where data from memory is stored
– the SMF (System Management Facility) datasets or log files
– the spool dataset, where the print queue is stored
– the JES checkpoint dataset
– the security software datasets

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

6) Other Considerations

Note that a weakness in the security software will undermine the security of MVS. And a weakness in MVS security will undermine the security software.

Hardware considerations such as shared storage devices and sysplexes will affect any mainframe audit, as described in our last issue.

The security software commands to list the options and rules are almost all TSO commands, that is, they are entered by means of the TSO (Time Sharing Option) online interface. If you are familiar with TSO, you might request a TSO userid with privileges that let it list (but not change) the security software rules. If this is not permitted, then you will need to rely on someone else to issue the commands for you. This may have implications for the quality of your evidence, but is sometimes the only approach possible.

In any case, there is no reason for any delay in your data gathering. Issuing any of these commands is a matter of a minute's typing. If there is a delay of more than a day between your request for this data and your receiving it, you may reasonably insist on faster responses.

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

6) Seminar Information and Miscellanea

6A) >>>>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** (October 29-November 1, 2013 in Chicago, and March 3-6, 2014 in Clearwater, FL)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (November 18-20, 2014 in Bethesda, MD), a logical follow-on to the previous course
- How to Audit **TCP/IP Security** (December 1, 2014 in Bethesda, MD)

To learn more about them, please go to

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

6B >>>>This Issue's Proverb of the Day

"*Behind every supposed audit finding lies an organizational issue that is the real finding*"
— Chinese Proverb

6C) >>>>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

6D) >>>>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 or Unsubscribe

Click on http://www.stuhenderson.com/subscribe.html
and follow the easy directions there.