MANEWS 11

the Mainframe Audit News

March 2009 Issue Number 11

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

Table of Contents

This issue of the MAN interrupts our scheduled description of how to conduct a mainframe audit in order to describe two new security features in z/OS: new tape dataset protection and digital signing of programs. In the next issue, we will resume out regularly planned audit program. In the meantime, this issue shows you how to think about these two new security features, what information to collect for the audit, and how to evaluate it for the audit.

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

1) New Ways to Protect Tape Datasets (and How to Audit Them)

With z/OS and the MVS operating system, there are now three tools to protect tape datasets:

- The security software (RACF, ACF2, or TopSecret)
- The TMS or Tape Management Software and
- Parmlib Members Named DEVSUPxx

The security software can use the same dataset rules that are used to control access to disk datasets to control access to tape datasets. Each of the three security software products has a switch with a name such as TAPEDSN to activate this protection of tape datasets. When this switch is set, the security software gets control every time a program opens a tape dataset, in order to decide whether to allow the program to read or write the dataset. (To “open” a dataset means that a program is asking the system to perform the housekeeping needed before the program can read or write the dataset.)

The **TMS** is software that maintains a database of every tape cartridge and the names of all the datasets on them. Examples of TMS products are: CA-1, TLMS, ZARA, Control-T, and DFSrmm. TMS software also gets control every time a program opens a tape dataset. When it gets control at open time, the TMS verifies that the correct tape has been mounted, and updates its database of tape information. The TMS can also call the security software to decide whether to allow the program to read or write the dataset. Each of the TMS products has a switch which the system programmer can set to tell the product whether or not to call the security software this way. ***So there are at least two ways to tell the system to call the security software*** for tape datasets: a switch in the security software and a different switch in the TMS.

The parmlib members named DEVSUPxx contain four operands which can also control tape security. (The parmlib datasets are the configuration files where the system programmer tells the system software which options to implement.)

They four operands are:

- **TAPEAUTHDSN** (= YES or NO, defaults to NO)
- **TAPEAUTHF1** (= YES or NO, defaults to NO)
- **TAPEAUTHRC4** (= ALLOW or FAIL, defaults to FAIL)
- **TAPEAUTHRC8** (= FAIL or WARN, defaults to FAIL)

The latter two only apply to security software calls caused by the first two.

TAPEAUTHDSN tells the system whether to call the security software for tape datasets. This is a ***third way to tell the system to call the security software for tape datasets***.

TAPEAUTHF1 can be used to tell the system or your Tape Management Software to call the security software for every dataset on a tape cartridge instead of just the dataset you are reading.

TAPEAUTHRC4 tells the system what to do if the security software is called by either TAPEAUTHDSN or TAPEAUTHF1 and the security software indicates "no dataset rule matches this dsname."

TAPEAUTHRC8 tells the system what to do if the security software is called either by TAPEAUTHDSN or TAPEAUTHF1 and the security software says to fail the request. This is like a warning mode, but just for tape datasets.

You can see that there are three different ways to have the security software protect a tape dataset:

- by a switch in the security software,
- by a switch in the TMS, and
- by the TAPEAUTHDSN switch in DEVSUPxx.

There are pros and cons to each approach. For your audit, you will need to collect the listings and switch settings to know which of these ways, if any, is being used. Tape datasets should be protected by the security software, by means of just one of the three possible ways.

But for foreign tapes, that is, tapes from other data centers with dsnames that don't match your naming standards and don't have security software rules, you might want to allow access to anyone. You could turn off the switch in the security software. You could then have the DEVSUPxx member of parmlib specify **TAPEAUTHDSN=YES** and **TAPEAUTHRC4=ALLOW**. Now the system will call the security software for tape datasets, but will allow any tape dataset access that has no matching dataset rule. In effect this allows access to any tape dataset which has no rule in the security software, but just for tape datasets. This might be exactly what you want to do.

Of course, you still need to get a check on the full 44 character dsname, so your Tape Management Software will have to be involved. And you need to control Bypass Label Processing. And you need to take care of residual data on tapes. But now you have more tools available to you.

For a mainframe security audit which includes tape datasets in its scope, you want to collect for your working papers:

1. The security software settings for tape datasets (in RACF, get **SETR LIST**; in ACF2, get a **SHOW ALL**; in TopSecret, get a **TSS MODIFY(STATUS)**)

2. The name of the tape management software (likely one of the five listed above) and a copy of the control file where its options are set

3. A copy of the parmlib members with names beginning DEVSUP..

4. Interview notes with security administrators, with TMS administrators, and with whoever administers DEVSUPxx.

Then determine: which switches are set to call the security software for tape datasets, how the 44 character dsname is checked, how tape Bypass Label Processing is controlled; and how foreign tapes are controlled. Verify your findings with data center staff and determine whether there is need for improvement in efficiency or security. Review your findings and recommendations with data center staff before going final.

For more information on mainframe tape security, please look at this article titled "**Full Tape Security from Security Software and Tape Management Software**": www.stuhenderson.com/TAPESEC1.PDF

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

2) New Security Features in Latest Release of z/OS

The latest release of **z/OS** (**1.11)**, the MVS operating system, and the RACF security software offers us new security features. (You will see generally see features in ACF2 and TopSecret that match all the important features of RACF). The most important for auditors include:

1. Identity propagation that lets subsystems on the mainframe associate userids on other platforms with RACF userids. You'll see this used first by CICS.

2. Programs can now be digitally signed, making it easy to tell when a program has been changed.

3. The ability to tell RACF that when a user first tries to use USS (UNIX under control of MVS), RACF should automatically assign the user a valid UID and GID. This should reduce the administrative effort required to create OMVS segments for users and groups by hand.

More information will be available on the details of each of these in the near future. However, one of these features is worth studying right now: **the ability to digitally sign a program.** This will be of critical importance in change control audits, and also in MVS audits, to be able to identify program modules which have been changed from what they should be. You will likely see in the near future software tools for auditors to take advantage of this to help you identify programs which have been modified improperly.

This digital signing of programs is based on the idea of a **unique number (called a "hash total") calculated for each program**. The hash total is then encrypted with the secret key of the vendor (IBM for example with z/OS software). To learn if a program has been modified improperly, you calculate your own hash total for the program and compare it to the hash total provided with the program. If the two hash totals are equal, you can then assume that the two versions of the program are identical, since a change to the program would result in the calculation producing a different total.

But then how do you know that the provided hash total hasn't been modified, along with an unauthorized modification to the program? By comparing the hash total you calculate to one you know you can trust (the standard). (Don't worry, there will be automated tools to do this calculation for you.) This standard hash total can be the one you calculated the previous year and kept in your work papers. Or it can be one you know came from a reliable source (such as the software vendor). You can demonstrate that it came from a reliable source if the source encrypted the hash total with its secret encryption key (using two-key or public key encryption, the kind that lets you encrypt with one number and decrypt with a different number)

If you know the public key of the source (say, the software vendor), you can use it to decrypt the standard hash total, and then compare the standard to the hash total you calculated. RACF, ACF2, and TopSecret all have support for storing these decryption keys in digital certificates, for calculating hash totals, and verifying their authenticity. If this sounds similar to the techniques Microsoft uses for digitally signing updates to their software, it is.

This has quite a few implications for the audit:

a. Vendors of software tools for automated work papers will want to consider enhancing their products to incorporate hash totals.
b. In your audit, you can calculate and compare a few hash totals yourself. Or you can review the procedures the data center uses for them to use hash totals to identify unauthorized changes to programs.
c. This will affect the change control software the data center uses, and the procedures they have (and which you audit) for them to control their own software.
d. This will also affect the change control procedures the data center uses (and which you audit) for them to control system software, such as the MVS operating system.
e. For the data gathering portion of your audit, you will want to collect information on the procedures and reporting the data center uses to take advantage of this digital signing of programs. In your analysis, you will

want to evaluate the degree to which management can rely on whether unauthorized changes would be prevented and/or detected.

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

3) Seminar Information and Miscellanea (Useful Articles, Proverb, Interesting Products)

3A) >>>>Seminar Information

_____

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

- How to Audit **MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (May 4-7, 2009 in Raleigh, NC, and November 16-19, 2009 in Clearwater, FL)

- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (June 9-11, 2009 in Bethesda, MD) and Sept. 15-17, 2009 in Bethesda, MD (a logical follow-on to the previous course)

To learn more about them, please go to

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

3B) >>>>Useful Articles

_____

How to Secure Mainframe FTP
is described in an article at http://zjournal.tcipubs.com/issues/zJ.Dec-Jan08.pdf in the **zJournal**.

21 RACF Tips

RACF is of course the security software for mainframe computers (it competes with ACF2 and TopSecret.) The handout from a recent ISACA presentation **"21 Things You Didn't Used to Know About RACF**" is available at:

www.stuhenderson.com/XARTSTXT.HTM

If you are involved in RACF audits, you should take a look. If you're involved in ACF2 or TopSecret audits, then you should look too, since the concepts apply (with different buzzwords) to those software tools as well.

Tape Security

To learn more about why tape security requires special efforts, you might want to read this article titled "**Full Tape Security from Security Software and Tape Management Software**": www.stuhenderson.com/TAPESEC1.PDF

3C) >>>>This Issue's Proverb of the Day

"*If it seems you are taking one step forward and two steps back, put it to music and dance*."

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

4) 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, OS/390, 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 Websphere server software which connects a mainframe to the Internet. (Note, we will expand each of these acronyms and explain how the software works over the course of the next several 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 for the Mainframe Auditors' Newsletter (MA News)

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