MANEWS 12

the Mainframe Audit News

July, 2009 Issue Number 12

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

Table of Contents

This issue of the MAN continues our description of how to scope and plan a mainframe audit, first started in Issue 10.

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

1) Scoping and Planning a Mainframe Security Audit (cont'd)

We started this discussion in Issue 10 (www.stuhenderson.com/MainframeAuditNews/MANEWS10.pdf), noting that planning and scoping is easier if you have a security model. Our security model for mainframes has two parts:

- The **Trusted Computing Bas**e (which relies on hardware controls and was covered in Issue 10) AND
- The **Q1Q2 Mechanism** which is the security software (always one of: *RACF, ACF2, or TopSecret*) which we address here.

As we discussed in Issue 10, when you plan your audit, you should make clear which of these two essential components you are addressing. You should also specify which MVS images (CPUs, LPARs, sysplexes) are included in your scope.

On the Q1Q2 mechanism: **Q1**, or Question 1, is "***Who is this user?***" and is often answered by means of a userid and password.

Q2, or Question 2, is "***Can this user do X?***", where X can be "open this dataset" or "execute this online transaction" or anything at all.

(Note on the concept of "*open a dataset*": When a program wants to do reads and writes to a dataset, the program must first "open" the dataset. This performs housekeeping functions to support subsequent read and write requests. The OPEN function calls the security software to provide dataset protection, refusing to allow reads and writes if the user is not permitted to the dataset. A "dataset" means the same thing as a "file".)

<table>
<tr><th colspan="5">Mainframe Security Audit Model</th></tr>
<tr><th colspan="3">Trusted Computing Base
(Issue 10 of this newsletter)</th><th colspan="2">Q1Q2 Mechanism
(This Issue)</th></tr>
<tr><td colspan="2">Hardware Controls, Which Restrict:</td><td colspan="2">MVS Operating System Use the Hardware Controls for Two Purposes:</td><td>Q1 (Who is this User?) based often on userid and password</td><td>Q2 (Can this user do x?) where x is open a dataset, issue a transaction, or anything you want</td></tr>
<tr><td>What Memory You Can Access</td><td>What Instructions You Can Execute</td><td>Keep Users from Interfering with Each Other</td><td>Keep Users from Interfering with MVS</td><td colspan="2">Always One of These Three Software Packages: RACF, ACF2, or Top Secret</td></tr>
</table>

If you come from a UNIX or Windows background, you may be surprised that the Q1Q2 mechanism is not part of the MVS mainframe operating system. It isn't. Instead data centers have to buy one of the three software packages that do the job. Of course in planning your audit, you should learn which of the three is in use

Whether you use RACF, ACF2, or TopSecret, both questions get answered essentially the same way. For Q1, imagine a user at a terminal, signing on to TSO with a userid and password. TSO calls the Q1Q2 mechanism, saying "Hey, security software, here's a userid and password. Tell me, who is this user?" All three security software products follow a similar approach (as do UNIX and Windows): They take the userid and use it as an index or key to read their database of user records, and to find the user record for that user. They then call the encryption routine to encrypt the password that was typed in, and compare the result to the encrypted password in the user record. If they match, and if some other tests are satisfied, then the security software allows the user to sign in. It copies most of the information about the user from the user record into a control block (formatted memory) called the ACEE. (ACEE stands for Access Control Environment Element. Aren't you glad you asked?)

The ACEE is the answer to the question "Who is this User?"

Now whenever the user tries to do something like open a dataset, the OPEN software calls the security software, pointing at the ACEE, and asking "Can this user open this dataset?" The security software goes to its database and finds a dataset rule that describes who can read or write that dataset. It compares what is in the rule with the ACEE (which describes the user) and returns a YES or NO answer.

For anything other than a dataset (for example an online transaction), the security software uses a resource rule instead of a dataset rule. Resource rules are very similar to dataset rules, and are processed in the same fashion to answer Q2. So when a user tries for example to execute an online transaction, the transaction management software will call the security software, pointing at the ACEE, and asking "Can this user do this transaction?" The logic used to answer Q2 is the same, whether the security software is using a dataset rule or a resource rule.

A note on SAF: **SAF** (System Authorization Facility) is the way a program invokes the security software, regardless of whether the software is RACF, ACF2, or TopSecret. When the security software starts up, it places the addresses of its Q1, Q2, and other routines into a table called the SAF Router Table. Now when some program wants to ask the security software to answer Q1 or Q2, the program calls SAF. SAF uses whatever addresses are in its table to branch to the security software. So you can think of "SAF" as a shorthand for "RACF, ACF2, or TopSecret, whichever one they have here"

So how do we apply this in planning and scoping our audits? Here's a checklist:

- Identify all the MVS images (CPUs, LPARs, sysplexes) and determine which are within your scope.
- Determine whether you will be addressing the Trusted Computing Base (see Issue 10) or the Q1Q2 mechanism, or both.
- If Q1Q2, then determine whether the installation uses RACF, ACF2, or TopSecret.
- Request BEFORE THE AUDIT STARTS, a listing of the basic options for the security software. For RACF, request both a **SETR LIST** and a **DSMON** report (all eleven sub-reports). For ACF2, request a **SHOW ALL** report. For Top Secret, request a **TSS MODIFY(STATUS**) report. File this in your working papers and get someone on your team to review it, summarizing how each of the critical options is set. (For RACF see the **ARTICLES** section of my website [http://www.stuhenderson.com] for explanations of SETR LIST and DSMON.)
- Request BEFORE THE AUDIT STARTS the naming conventions for datasets, online transactions, and other items. For example, any dataset whose name begins **SYS1.** will probably be a system dataset.
- If the Trusted Computing Base is within your scope, request copies of the security software dataset rules for all datasets where backdoors can be defined. This will include the parmlibs, the APF authorized datasets, and others. You want to see from these rules who can update these datasets, and whether such updates get logged. Get the dataset rules also for the SMF datasets (log files) and the security software databases to see who can read and write them.
- If the Q1Q2 mechanism is within your scope, pick a few production applications ask for copies of their dataset and resource rules. You want to see who can read and who can write to the applications' datasets. Be prepared to evaluate these rules to determine whether they are what they should be. (What standard will your compare them to?)

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

2) How to Anchor the IS Audit

It sometimes happens that an IS audit loses focus and fails to concentrate on its control objectives. This is when auditees start asking "So what?" to your audit findings, which is always irritating.

A good way to maintain focus (and to avoid wasting time and energy on data-gathering and analysis that isn't needed) is to anchor the IS audit in the financial

audit. Most IS audits are providing support for, or are otherwise connected to, a financial audit. And most financial audits address one or more of these control objectives:

a) Reliability of the numbers (financial, inventory, sales, other)
b) Protection of assets (including information assets and information processing assets)
c) Going concern
d) Compliance with laws and regulations

You can use these to maintain focus. For every data-gathering and analysis step you take, ask yourself, "How does this support the financial control objectives, and if it doesn't, then why am I doing it?" The result will be faster, more efficient, and better received audits.

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

3) What is FISCAM and Why Should I Care?

FISCAM (Federal Information System Controls Audit Manual) documents the approach to be used for IS audits of Federal agencies of the US government. It is of course useful to know if you will be auditing government agencies, or regulated industries such as health care, or any industry which takes funds from the Federal government. But because the methodology it documents includes a solid, organized approach to evaluating IS controls, it will be useful in non-governmental audits. You will be a better auditor, and you will improve your own audit approach, if you read this manual. It is available at:

www.gao.gov.new.items/d09232g.pdf

Incidentally, this document describes several control tools which will help IS managers to do their job well.

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

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

4A) >>>>Seminar Information

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

- How to Audit **MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (November 16-19, 2009 in Clearwater, FL)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (September 15-17, 2009 in Bethesda, MD and April 12-14, 2010 in Bethesda, MD), a logical follow-on to the previous course
- (NEW) **Effective FISCAM Audits of Mainframes with z/OS and MVS** (November 10-12, 2009 in Bethesda, MD)

To learn more about them, please go to

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

4B) >>>>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

4C) >>>>This Issue's Proverb of the Day

"*The idea that seeing life means going from place to place and doing a great variety of obvious things is an illusion natural to dull minds*." -- Charles Horton Cooley

4D) >>>>Interesting Products

While we seldom recommend products, we think these two software products are worth your taking a look to make your own evaluation.

- Brand new product! **CA Compliance Manager for z/OS** helps organizations easily manage and audit their mainframe environment elevating compliance management, analysis and reporting to a new level. CA Compliance Manager provides for the collection and alerting of compliance-related information and events occurring within your mainframe environment while running 100% on platform and web browser based. CA Compliance Manager helps you continuously monitor, detect, collect, and report changes to data, operating system, and security product configurations by defining policy to capture the real-time information that you deem critical for on-going compliance activities all without having to rely on SMF logs or other manual processes. For more info, please contact Carla.Flores@ca.com or Rana.Zayed@ca.com .

- **CA Cleanup (for CA ACF2, CA Top Secret or IBM RACF)** automates two labor-intensive tasks that plague security administrators: creating security commands to remove obsolete IDs or access, and creating commands to restore

what was removed. When using CA Cleanup, you can easily identify active and inactive user IDs, profiles and permissions, as well as user-defined resource classes For more info, please contact Carla.Flores@ca.com or Rana.Zayed@ca.com

- **NEON zPrime** is an innovative new product that facilitates the movement of mainframe application processing from expensive central processors to low-cost specialty processors, reducing the cost of mainframe computing by up to 20%. IBM introduced specialty processors as a way of lowering the cost of mainframe computing and making it more competitive with midsize server solutions. In 2004, IBM introduced the System z Application Assist Processor (zAAP) to reduce the cost of hosting web-based applications on the mainframe, and then in 2006, IBM introduced the System z Integrated Information Processors (zIIP) to help defray the cost of DB2 application processing. zPrime expands the use of zAAPs and zIIPs to IMS, CICS, DB2, TSO/ISPF and batch application processing. This work is typically 75% of the work processed on a mainframe. Users of zPrime are able to move up to 90% of specific application workloads to zIIPs and zAAPs, resulting in significant cost savings – which can be several million dollars annually. For more info, please contact Robin Reddick: Robin.Reddick@neonesoft.com. Or visit www.neon.com.

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

5) 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.)

MANEWS 12

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
