MANEWS 15

the Mainframe Audit News

June, 2010 Issue Number 15

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

Table of Contents

This issue of the MAN explores the value of poking around

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

1) Poking Around

Here are four stories, each involving a different type of knowledge: You will be a better auditor by seeing the different types of technical knowledge involved. But you will also benefit by noting what the stories have in common.

First, an auditor performing a **security audit of CICS** on a test system happened to type in the name of a sensitive transaction. He did this after connecting his terminal to the CICS region, but BEFORE he had logged on with a userid and password. The transaction started to execute. He immediately killed it before it actually did anything. The transaction is not supposed to execute under these conditions of course. CICS is known for its philosophy of "You can't do anything unless the security software has proved who you are.".

He asked various technicians how this could have happened and received shoulder shrugs as responses. He eventually learned what had come about: Each CICS region has a **default userid** specified (in the **DFHSIT control file**, which belongs in your working papers for a CICS audit. More on this in a future issue.)

CICS uses this default userid to call the security software whenever CICS needs a security answer and doesn't have any other verified userid to work with. In this example, the default userid had been inadvertently permitted to the sensitive transaction.

When our auditor typed the name of the transaction without having logged on, CICS used the default userid to call the security software, asking "Can this user do this transaction?". The answer was "YES", so CICS started the transaction executing.

Our auditor would not have discovered this security weakness if he had only followed the audit procedure he was supposed to use to audit CICS. He now checks what transactions the default useid is permitted to, in addition to his prescribed audit steps.

He also followed up by reviewing the approval and re-certification procedures that had resulted in this situation. ("***The technical stuff is easy. But there's always an organizational issue behind any technical issue***.")

Our **second** story involves a different auditor working on a mainframe **security audit involving two lpars** (virtual or "pretend" CPUs defined on the same "real" CPU). Each lpar ("logical partition") of course had its own copy or "image" of the MVS operating system.

One MVS image was used for Testing and Development while the other was used for Production. While both images used TCP/IP to connect to the Internet, our auditor received assurance that the firewall involved made it impossible to access the Production image from the Test image.

Running some random tests, our auditor happened (partly by chance, partly by deliberately attempting various combinations of access attempts) to try pinging the Production image from the Test image. The ping succeeded. He also asked various technicians how this could have happened and received many responses of "This couldn't have happened.". But it did.

He eventually learned that there was a hardware device called an OSA adaptor in the TCP/IP network used to connect the firewall to the MVS images. In this case, to speed up performance, the OSA had been configured with a standard option that happened to permit access from one side to the other. Because the two MVS images connected to the OSA before reaching the firewall, the OSA then bypassed the firewall's separation of Test from Production.

His standard audit procedures would not have identified this exposure, in fact did not address the issue of OSA's and how they can be shared between lpars at all. He now checks for shared OSA's (and shared disk drives and other shared hardware) in addition to following the steps in his standard audit procedure.

He had discovered a whole new layer of technology (the **HCD** or **Hardware Configuration Definition**) for mainframe computers. This is where lpars are defined, as well as sysplexes and shared devices such as OSAs and disk drives. (Can you see if two lpars share a disk drive containing a sensitive dataset, how the scope of the audit could be affected if each lpar had its own RACF database with its own dataset rules?). He now excludes the HCD from the scope of his mainframe audits unless he has the resources to evaluate it effectively.

Our **third** auditor was evaluating the controls over a financial application on a mainframe. He happened to create his own list of input files, and wandered around verifying where each came from. He discovered one critical set of files came not from within the data center, but from spreadsheets maintained on personal computers in one user department. The documentation for the application did not list the personal computers, nor how the files were input to the application.

Looking further into the matter, he discovered that some of the data quality controls which were in force in the data center were not in force on the personal computers. To no one's surprise, further checking revealed problems with the quality of the data. This discovery of course had an effect on the financial audit.

This auditor now pays greater attention to the scope of application controls, and to the boundaries between the mainframe data center and its data sources. He recognizes that while he still needs to make use of his standard audit procedures, he can augment them by poking around to see what he finds. He also realized how useful it is to have knowledge of financial applications and how they function.

Our **fourth** story involves not an auditor, but rather a knowledgeable MVS system programmer. He wondered how much he could trust the security of several purchased software packages which required the privileges of the MVS operating system to function. He wrote programs which automatically called the software with random combinations of input and then observed the resulting output. He discovered several software products which contained security flaws which any TSO user could have used to bypass the system's security.

Because he wore a white hat, this system programmer quietly contacted the software vendors involved and informed them of what he had found, so that they could fix the problems before anyone else found out. (Wouldn't it be great if this system programmer would run his tests of every major mainframe software product and give us a "seal of approval" for ones without identified security holes?)

This story required deep knowledge of MVS internals and automated program testing techniques.

Unlike the first three stories, this one involved deliberate generation of every possible combination of inputs, with automated checking of the results. This is a systematic way of poking around.

Of course poking around to find unexpected discoveries is what these stories have in common. They differ in the technology involved (CICS internal logic, hardware configuration, flow of files within an application and data center boundaries, and system software internals), but share the concept of poking around.

What can we learn from this? While standardized checklists and audit procedures will always be needed to guide us, they cannot possibly address every issue we might encounter. This suggests that we should be extremely careful in our scoping.

It also suggests that we should be aware of the technologies involved in our audits, and try to learn something about them before the audit begins.

It also suggests that we should try poking around a bit whenever we can. Does you last audit's budget have a line item for poking around? Do you wish it had?

And this leads us to the question of how to poke around safely. Some data centers refuse to give auditors userids with access to the system. This makes it more difficult to perform direct collection of audit data. This also protects you from (accurate or inaccurate) charges of damaging a system. When you do have access to a system, you want to be careful what commands and transactions you try to execute. When you don't have direct access to a system, you can often arrange to "shoulder surf", observing an authorized user while he pokes around for you.

(Editor's note: some of the details in these stories may have been sanitized to protect personally identifiable information. No Essential Truths were harmed in the production of this article.)

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

"***If an audit has to be boring, then I'd rather be working an assembly line***"

2) Seminar Information and Miscellanea (Useful Articles, Proverb)

2A) >>>>Seminar Information

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

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

- **Comprehensive IS Auditing with Case Studies** (July 19-20, 2010 in Bethesda, MD; and November 4-5, 2010 in Bethesda, MD)
- How to Audit **MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (November 16-19, 2010 in Clearwater, FL)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (April 6-8, 2011 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

2B) >>>>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**.

FISCAM (Federal Information System Controls Audit Manual) documents the approach to be used for IS audits of Federal agencies of the US government: www.gao.gov.new.items/d09232g.pdf

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

2C) >>>>This Issue's Proverb of the Day

"*There are two things every manager needs to do: first, set up a series of low overhead automatic measurements that tell him when something needs attention (and only bothers him when something DOES need attention, and second, occasionally to walk around his operation observing what is happening and talking to employees at every level. Only then can he expect to know what he needs to know."*

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

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 will expand each of these acronyms and explain how the software works over the course of 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 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