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

M A News
Mainframe Audit News
April, 2007
Issue Number 08

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

Table of Contents and Introduction to the Mainframe Audit News

1) Introducing the Mainframe Audit News

This is the eighth edition of the Mainframe Audit News, a vehicle for sharing information about auditing IBM mainframe computers. For more information on this newsletter, including how to subscribe or un-subscribe, please see section 5.

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

2) New RACF Tips for Auditors and Info on Tape File Security

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 from the zSystems Journal, titled "**Overcoming the Challenges of Tape Security in a Mainframe Environment**":

www.zjournal.com/index.cfm?section=article&aid=762

3) Mainframe Audit Checklist and Testing What You Have Learned

Mainframe Audit Checklist

The recent exposure of large numbers of credit card numbers and other sensitive data resulting from incomplete security makes many of our managers wonder how secure we are. Here is an outline, and partial checklist, to organize your thinking as you prepare to answer the inevitable questions about mainframe security. Each Roman number below could be addressed as an individual audit. References to other issues of this newsletter are in [square brackets].

I **MVS security** [Issue #1] ("Backdoors" are techniques that let system programmers give certain programs privileges which let those programs bypass all security on the system. Examples of backdoors include the Program Properties Table, User Supervisor Calls, and APF Authorization.)

--- What backdoors exist on the system?

--- Who can modify them and would it be logged to SMF?

--- Would management be aware of any unapproved modifications?

--- How well does IT management know that only approved backdoors are there?

--- How well does IT management know that the approved backdoors are safe?

--- How well does IT management know that the backdoors can't be modified improperly?

II Access to the System and Proving Each User's Identity [Issue #3]
(On the mainframe, these controls consist of one of the three security software products: RACF, ACF2, and TopSecret. These products verify users' passwords and restrict access to the system. They also control access to datasets and resources.)

--- Which security software is in use?

--- Does it control every path into the system (TSO, Started Tasks, Batch jobs, NJE, RJE, USS, TCP/IP, applids)

--- Does it reliably verify each user's identity (all the issues regarding password length and change frequency, userid and password administration and related topics)

III Access to Data [Issue # 3]

--- Does the security software properly restrict access to data on disk?

--- To data on tape? (Include tape management software in the assessment)

--- Is the ability to bypass label processing on tapes controlled?

--- Is the ability to store two files with dissimilar security requirements on the same tape cartridge restricted?

--- Does the security software properly restrict access to printouts in the print queue, waiting to be printed?

--- Does the security software properly restrict access to residual data on both tape and disk?

--- Is all sensitive data encrypted whenever it leaves the data center? (for example, when a backup tape is shipped to an offsite storage facility or a critical file is sent to a business partner by tape or over the Internet)

--- Are privileges that permit a user to access any dataset limited to an approved set of users?

IV **USS (UNIX) Security** [Issue #2]

--- Are the numbers that identify users and groups of users (**UID**s and **GID**s) well managed so that there are no non-deliberate duplications?

--- Is USS file security based on **EXECUTE** permission to directories and sub-directories?

--- Are mounted file systems security options set securely?

--- Are security software rules in the **UNIXPRIV** resource class set securely?

--- Are security software rules in the **FACILITY** class with names starting **BPX**. Securely defined?

V **TCP/IP Security on the Mainframe** [Issues #4 and #7]

--- Use the **NETSTAT** command to learn what programs are running on what ports and what IP addresses.

VI **Non-TCP/IP Network Security** [Issue #7]

VII **Middleware such as CICS, IMS, DB2, MQ Series, and others** [future issues]

VIII **Controls Over Security Decision Making**

--- Is someone other than the security administrator clearly responsible for deciding who can read and who can write each application's files?

--- For deciding who can have a userid?

--- For deciding who can have privileges such as **OPERATIONS** or **NON-CNCL?**

--- For deciding which resource classes and types are to be controlled and what the rules should be?

--- Are these decisions in writing?

--- Do these decisions match the rules in RACF, ACF2, or TopSecret?

--- Are these decisions made by the persons who best understand the associated business and operational risks and regulations?

--- Can the case be made from written documentation that the access rules protecting data are what they should be? (that is, that they match the decisions of the people who best understand the risks)

--- Does the security administrator have the authority to say **NO** when high level managers demand access for their staff without getting written approvals?

Testing What You Have Learned

In earlier issues, we defined and explained each of these terms. How many of them can you define? (This quiz is open book.)

a) APPLID
b) MQ Series
c) TCP/IP
d) USS
e) VSAM
f) HLQ
g) System Symbol

4) Seminar Information, and the Proverb of the Day

4A) >>>>Seminar Information

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

- How to Audit **MVS, RACF, ACF2, CICS and DB2 Security** (May 7-9, 2007 in Raleigh, NC and November 14-16, 2007 in Clearwater, FL)

- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (May 16-18, 2007 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

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

_____

“If what you’re doing isn’t working, then try something else.”

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

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.)

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

_____