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

M A News
Mainframe Audit News
May, 2005
Issue Number 07

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

Table of Contents

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

1) Introducing the Mainframe Audit News

This is the seventh 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) More on Mainframe Networks

Continuing our discussion of mainframe networks in the last issue, there are two types of mainframe network:: SNA and TCP/IP. Most mainframes will have both, requiring separate audits.

SNA (**Systems Network Architecture**) Networks

SNA networks are the original type of network for mainframes. They provide a tightly controlled environment for high volume transactions. They use an architecture developed by IBM, which supports various protocols for different devices and for different types of software. In the past, translation among these protocols often

took a lot of time and resources. So IBM eventually developed the APPC **(Advanced Program to Program**) protocol as a standard which could be used by all hardware and software over SNA networks. APPC is sometimes referred to as **LU 6.2**. It provides the basis for secure communication between two programs on different types of computer, and between SNA networks connected together.

TCP/IP (**Transport Control Protocol / Internet Protocol**)

TCP/IP networks were originally developed for UNIX computers, spread to the Internet, and now are supported and recommended for Windows and Novell networks as well. IBM now supports both SNA (including APPC) and TCP/IP on the mainframe.

Which Way is the Mainframe Going?

Some people believe that TCP/IP is pushing SNA and APPC off the mainframe. Others believe that SNA will always rule on the mainframe. In real life, you will find that most mainframe installations have both SNA and TCP/IP. When a large financial institution hooks its network up to that of another financial institution, the networks are usually SNA networks. Last issue of this newsletter discussed a serious security issue you need to address if your SNA network is connected to other organizations' networks. This exposure can be managed by using the security provided by APPC to verify the identity of computers in other networks.

When terminals are connected to the mainframe, they are most likely to use a TCP/IP connection. We hope to convince you that this is the most secure, most reliable, most scalable, most flexible, and most standard TCP/IP you will find anywhere, if you implement the available tools properly. (It took IBM a few tries to get it right, but TCP/IP on the mainframe is now all these things and more.) Part of the auditor's responsibility is to help ensure that the available tools are effectively used.

How TCP/IP Works

TCP/IP uses IP addresses for routing of messages. (Each IP address consists of four numbers separated by dots, for example: 192.168.23.1) Each IP message can contain a TCP packet.

Each TCP/IP packet contains a port number, which identifies the application which handles the packet. So when an IP message comes into the mainframe, VTAM receives it, recognizes it as IP, hands it to IP, who recognizes if it is

TCP, and hands it to TCP. The TCP software looks at the port number and hands the packet to whichever program handles that port number's application. For example, port number 25 is often for email, port 23 for remote logon, and ports 20 and 21 for FTP or File Transport Protocol.

Each of the TCP/IP applications is a started task (a batch program started by an operator command). For your audit planning, you can issue the TSO command NETSTAT. This will tell you what ports are being used and what application program is supporting each one.

One Example: FTP:

One of these applications will likely be FTP (File Transport Protocol), used to upload and download MVS datasets and USS files. On the mainframe, it can also be used to talk with DB2 (database software), to submit batch jobs, to download printouts, and to issue operator commands. As an example, here is a list of the security tools IBM makes available to us to secure FTP on the mainframe:

- Control over use of ports, by means of FTP control statements, firewalls, and security software
- Use of SSL (Secure Sockets Layer), TLS (Transport Layer Security), and Kerberos both to provide encryption and to verify users' identities
- Use of exits (programs to alter the logic of FTP) to add custom security
- Calls to security software to control who can use FTP, and what IP addresses they can connect from
- Control over anonymous logons, and assignment of default identities
- FTP control statements to restrict access to JES (Job Entry Substem, software which manages batch jobs for MVS) and to DB2 (database software).

You might address all of these in an FTP audit, perhaps as a result of the NETSTAT command informing you of significant FTP usage. The data-gathering for your audit would include: the TCP/IP control file; the FTP control file; security software rules for these resource classes: SERVAUTH, APPL, TERMINAL, and FACILITY, as well as for userids, digital certificates, and keyrings; copies of exits; and summaries of firewall configurations.

If you have sensitive or critical applications executing on your mainframe, and if the capability exists to upload and download mainframe files from the Internet, you might consider it worthwhile to review the controls over FTP access. With the available tools properly implemented, this will be the most secure FTP anywhere.

If you wanted to segment your mainframe security audit activities in order to do just a portion each year, you might organize them into these groupings:

- Trusted Computing Base (MVS security) (described in earlier issues)
- Security Software (RACF, ACF2, or TopSecret) and Tape Management Software
- Middleware such as DB2, CICS, and MQ Series
- Networks

Within Networks, you might address SNA and TCP/IP networks separately. Within TCP/IP, you might address each of the applications (such as FTP) separately.

3) What to Say to the System Programmer and Testing What You Have Learned

What to Say to the System Programmer who wants to know what your MVS security audit is all about:

"I've been asked to evaluate the controls available to IT management to let them know that each back door to MVS:

- Has been approved
- Is safe (doesn't permit unauthorized programs to obtain the privileges of MVS, and thereby bypass all the security on the system)
- Has not been modified / Cannot be modified improperly

Without such controls effectively implemented (and documented), we cannot rely on the security of any application executing on the mainframe. This affects the degree to which we can rely on financial and other applications providing valid data. Further, if your business is dependent upon mainframe applications, then this affects how much investors can expect you to be in business in the future."

Testing What You Have Learned

In Issue 03, we described **Job Control Language** or JCL, including the **EXEC card** which describes a program to be executed (usually followed by **the DD (data definition) cards describing the datasets to be used by the program**). Below is a partial sample of a DD card. How many of the following questions can you answer?

//INFILE2 DD DSN=STU.TESTDATA, DISP=(OLD,KEEP),LABEL=(2,BLP)

Questions:

1) What is the DDNAME of this dataset?
2) What is the DSNAME of this dataset?
3) Is this an existing dataset or a new one? What will be done with it after the program runs?
4) Is this a tape dataset, a disk dataset, or a printout?

4) Seminar Information, and the Proverb of the Day

4A) >>>>Seminar Information

This issue we highlight a special session of a popular mainframe audit seminar, scheduled for July 19-21, 2005 in Dallas, TX

:

- How to Audit **MVS, RACF, ACF2, CICS and DB2 Security**

The next public session of this class after that will not be until November 2-4, 2005 in Washington, DC.

To learn more about it, as well as our other “How to Audit…” seminars, please go to

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

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

(Source Unknown) "If you can’t explain it on a cocktail napkin, then you don’t understand it yet." (applies to audit findings, too)

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

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.

5A) >>>>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

5B) >>>>To Get Questions Answered from 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 the word: Question: (followed by your question, and tell us whether you want your name included or not if we decide to publish your question and answer) Whether we print your question and answer or not, we will try to email you back an answer to your question within five business days. If you need a faster answer, please phone your question to (301) 229-7187, leaving the question on the machine. Please repeat your phone number slowly and clearly.