MANEWS Issue Number 18

the Mainframe Audit News

Since our last two issues dealt with auditing CICS, this issue we address the related topic of auditing DB2 security. We also cover scope control for application audits and residual data on disks.

Table of Contents

1) New DB2 Security Features

DB2 (IBM's strategic database management software) has new security features that fix some major architectural problems with DB2 security. We'll describe a little bit about what's going on and what auditors need to know, and then we'll point you to a free white paper that has much more detail and useful advice.

Problems with DB2's Security Architecture

. Users are represented in DB2 by **authIDS** (authorization identifiers) which are similar to userids. Users don't log onto DB2. Instead, when a user connects to DB2, DB2 calls one of two programs to build the list of authIDs which constitutes the answer to the question "Who is this user?" These programs which build the list of authIDs are named **DSN3@ATH** and **DSN3@SGN**. The list of authIDs they build may include the security software userid of the user. In some cases the list of authIDs includes some other value, such as the name of a CICS transaction. When this happens, the identity of the user would be lost because the user was identified by the name of the transaction he was executing, not by his userid.

A second problem resulted from the architecture of the security tables which DB2 used to control access to data. Each row in these tables consisted of the granting of some permissions to some authID for a single table or other entity. There was no way to use wildcard characters to grant permission in a single row to a bunch of tables with similar names. This meant that for each authID, there would be one row in the security tables for every table to which it was granted access. This made it difficult to implement security precisely without a large number of rows in the security tables. It was common for auditors to discover that standards and administration procedures for these security tables were not documented. In some installations, auditors found that the permissions which had been granted were seldom reviewed for correctness, nor reviewed with application owners.

A third problem that impeded DB2 security administration was a feature called **cascading revoke**. Imagine that USERA grants a privilege to USERB who grants it to USERC who grants it to USERD. If the privilege is revoked (taken away from) USERA, then the cascading revoke feature automatically revoked the privilege from the other users. In some instances, when this happened, it was discovered that, no one had written down what the privileges were supposed to be, causing much difficulty in restoring things to normal.

A fourth problem with DB2 security involved separation of duties. Privileges such as SYSADM and DBADM gave a user both administrative power and complete access to data. This meant that it was not possible to separate system administration from security administration from access to data.

Improvements Over Time

Eventually it became possible to replace the security tables with calls to RACF, ACF2, or TopSecret. This greatly improved the situation, since the security software can use wildcard characters to secure many tables with a single rule.. However, not every DB2 installation has been converted this way, One of your first questions in a DB2 security audit might be "***Are you using the internal security tables in DB2 or are you using the security software for DB2 security?***".

Until recently, DB2 security still suffered from problems with separation of duties.

DB2 security audits often consist of review of how users are identified, and of how access is granted, either in the security tables or in the security software. Once an auditor has determined how many DB2 subsystems there are (production, test, etc.) and which are to be included in scope, then data gathering would start with acquiring a copy of DSNZPARM for each subsystem in scope. **DSNZPARM** is the module where each subsystem's options are set. These options include: specification of the "**install SYSADMs**" (emergency authIDs that have complete access to the system), whether the security mechanism is active, a default authID, and whether the DB2 subsystem can talk over the network to other computers. A copy of DSNZPARM belongs in the workpapers of every DB2 security audit.

More recently, IBM has added significant new security options to DB2, many of which are specified in DSNZPARM. Our audit programs will need to address these improvements.

The New Security Features for DB2

These features include: role-base security administration, options set in DSNZPARM, and new privileges that can be assigned to authIDs. The role-based security administration consists of definition of roles (collections of privileges), and assigning authIDs to the roles. Each authID participating in a role inherits all the privileges of the role.

With the latest releases of DB2, these new options are specified in **DSNZPARM**:

- **SEPARATE_SECURITY** addresses the problem with separation of duties. If this is set to YES, then the SYSADM privilege no longer grants access to data nor the ability to perform security administration. At the same time, three new privileges become active:

- **SECADM** for security administration without data access and
- **DATAACCESS** which gives complete access to application data without the ablity to perform security administration and
- **ACCESSCTRL** which gives a subset of the SECADM privilege

- **SECADM1** and **SECADM2**, the two authIDs or roles that automatically have the new SECADM privilege. This means that they can perform security administration without having access to data, but only if SEPARATE_SECURITY is set to YES.

- **SECADM1_TYPE** and **SECADM2_TYPE** (set equal to either AUTHID or ROLE) specify the type for SECADM1 and SECADM2

- **REVOKE_DEP_PRIVILEGES**. If set to YES then the cascading revoke feature is active (except for when the privileges ACCESSCTRL, DATAACCESS and system DBADM are revoked). If set to NO, then the cascading revoke feature no longer applies unless specified explicitly on the REVOKE statement. If set to SQLSTMT, then the cascading revoke depends upon the REVOKE statement in SQL.

We've given you a brief overview of DB2 security and its new features. You can learn a much more complete description (along with an outline for an audit program for DB2 security) from this free white paper: http://www.stuhenderson.com/NewDB2.pdf .

(Downloading the paper does **NOT** require that you provide your email address or any other information.)

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

2) How to Manage Scope on an Applications Audit

So you've started an applications audit, perhaps of General Ledger. You've narrowed your scope to just the security and reliability of the General Ledger production application. (The financial auditor has asked you to confirm that the numbers for the financial statement stored on the mainframe can be relied upon.)

You might be concerned that there might be an unreliable input. (You had heard about a GL audit where the auditor discovered an undocumented input, which turned out to be manually generated numbers which were discovered not to be reliable.) You want to be sure that your scope properly addresses all the inputs and their reliability.

One approach is to use a tool from systems analysis called an **IPO diagram**. This is not an Initial Public Offering of stock. IPO stands for Input-Process-Output. You draw a rectangle in the middle of a sheet of paper, labeling it: Process: General Ledger Program. You then list all the inputs on the left, with arrows pointing to the process rectangle. You list all the outputs on the right, with an arrow pointing from the process to each output. The purpose of the IPO diagram is to help confirm that you are addressing all the inputs, all the processes, and all the outputs.

If you want, you can list all the steps of the GL application inside the process rectangle. (A systems analyst would break these into their components using a formal process called functional de-composition, in order to understand the details that make up the process, and then improve them. You could use the same approach for an application whose logic you needed to address in an audit.)

To address the inputs to the GL process, your audit planning needs two steps:

a. Ensure that you have identified all the inputs and
b. Either evaluate the reliability and completeness of each input OR exclude the data quality for that input from your scope

To know that you've identified all the inputs, you'll consult the application's documentation. You might want to ensure that the data center's policy requires all inputs and outputs to be documented for each production application. If you want further confirmation, you might review the **JCL** (Job Control Language) for the application. The **DD** (Data Definition) statements there tell the computer what datasets to make available to the program as it is executing. If you want even further confirmation, you can review the **SMF** (System Management Facility) log file, which should have a record describing every file that the program uses as it is executing.

To evaluate the quality of the input data, you will either rely on controls outside the scope of your audit or consider conducting your own tests. If an input file is created by some other application, you may decide to rely on the audit for that application, and on the audit of the data center's data quality and change management controls. If you discover an input to the GL application that is not covered by some other audit, you might include tests in your own audit of the quality of the input data.

If you can't do either (rely on some other audit or perform sufficient testing as part of your audit), and if the input is material to the application, then you may need to state this in your audit report.

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

3) Connection Terminology You Need to Know

One of the foundation elements of any mainframe installation is the set of files that define the hardware, including which hardware elements are shared, and which are connected to each other. These files, which have no analog in the distributed world, are called the **IODF** (Input Output Definition Files). They are essential to a comprehensive audit since they dictate the paths across which data can be shared in a mainframe data center.

To emphasize the importance of these connection and sharing features, we introduce some terms you should be familiar with. These terms all deal with connectivity features that make the mainframe the most reliable and flexible platform available. You will see in the following paragraphs why they all have important implications for mainframe security audits.

LPAR — (Logical Partition) This is a logical (think pretend or virtual) splitting of a CPU (Central Processing Unit, the part of the computer that does logic and arithmetic) into two or more partitions. Each partition appears to be its own CPU, with its own copy of the operating system. (The operating system could be MVS, or VM, or LINUX.) The partitions on a given CPU are isolated from each other. This means you can run a test system in one LPAR and a production system in another LPAR on the same CPU while maintaining separation between test and production.

(If you think this is a form of virtualization, you are correct. LPARs are virtualization in the hardware. The VM operating system on the mainframe and VMware on distributed systems are software based virtualization. One major advantage of virtualization is that it permits load balancing of CPU resources.)

When you are trying to scope your audit, you might ask "How many CPUs in this data center?". The answer might be *"Well, there are five CPUs, but they're configured into fifteen LPARs*.", with a pause to see if you understand the word "LPAR". Your response could be: "*Oh, then there must be fifteen MVS images. I need to pick one of them that is a production MVS system running an important application. Which ones are production, and which one do you think I should base my audit on?"*

Sysplex — This is a collection of CPUs that are connected by fiber optic cable, often with large data storage devices called **coupling facilities** in-between. The CPUs can signal each other and can pick up each other's workloads. They can also use the fiber optic cable to mirror a database on one CPU with another copy of the database on one of the other CPUs.

You can see the access control implications: Suppose two databases are mirrored across a sysplex. Assume that each CPU has a different security software rules database. Then a change on the first copy of the database could be reflected in the second copy of the database in violation of the security rules on the second CPU. There is no right or wrong here. But to perform a comprehensive audit, you need to be aware of the possible risks in such a situation, and be prepared to address them.

IBM states that with a properly configured sysplex, you should expect no more than 4 or 5 minutes of unscheduled down time **PER YEAR**. (Emphasis added)

Shared DASD (Direct Access Storage Device, a fancy word for a disk drive) ---

Shared DASD is a physical connection of a disk drive to two or more CPUs or LPARs. This has no security implications if the two CPUs share the same security software rules database.

On the other hand, imagine a DASD shared between a test CPU and a production CPU. The DASD happens to have sensitive datasets on it. The two CPUs have different security software databases. The auditors check the dataset rules in the security software on the production system. If they don't check the test system's dataset rules, they might miss the fact that, for example, the test system rules permit every programmer to update the sensitive datasets.

What to Do

So you're planning a mainframe security audit, and you want to know what LPARs, sysplexes, and shared DASD might be involved. How can you learn how all this hardware is configured?. You have three possible sources:

a. Ask the system programmer for a map of CPUs, LPARs, sysplexes, and shared DASD. Rely on the information he provides.

b. Learn to read the control file where the hardware configurations are defined. This is called the **IODF**, or Input Output Definition File. The IBM manuals describing this are downloadable in pdf format from the Internet for free. Look also for manuals describing the **HCD** (Hardware Configuration Definition) menus and how they work to maintain the IODF.

c. Use software tools such as IODF Explorer from NewEra (www.newera.com) . (We know of no other tools that perform this function, but would be glad to mention any reliable other product that does.)

4) Residual Data

When a disk dataset is erased, the data is still there. Only the pointers to the data actually get erased, unless additional measures are taken. These measures might include either obllterating the data, or encrypting it. The "*data that is still there*" is called "***residual data***". If it is sensitive, it can represent a security risk.

The risk is that once the pointers get erased, that part of the disk drive is available for re-use. The next program to allocate (or create) a dataset on the same part of the disk drive will then be able to read the data. If I have TSO access to a system and want to get a copy of the customer master file, all I have to do is wait until just after the file gets erased. I then run a program that allocates large datasets on that disk drive, and I will be able to copy the residual data. This applies to credit card information, health information, personal information, and any other sensitive data.

Mainframe security software has options to protect residual data on disk. When these options are in effect and a disk dataset is erased, zeroes are written over the data before the pointers are erased. (RACF calls this feature **EOS** or **Erase-On-Scratch**. You can see whether it is set in the SETR LIST report. ACF2 and TopSecret call this feature **AUTOERASE**. You can see whether it is set in the ACF2 SHOW ALL report and the TopSecret TSS MODIFY(STATUS) listing.)

Many installations do not use these features to protect sensitive residual data. This may be because the system programmer believes that these features have serious performance problems. (This was true in the last century. The performance problems have been resolved in several ways, described below.)

In other installations, sensitive residual data is not protected because it is apparently no one's job to protect it. This is a question of IT governance. The RACF/ACF2/TopSecret administrator does not have the knowledge to determine which datasets are sensitive. The Compliance and Legal departments should have this knowledge. You will likely have an audit recommendation to make unless the following are all true: Compliance, Legal, and application owners determine specifically which files are sensitive and why. They provide this information to the security administrator. The security administrator in consultation with the system programmer implements protection over residual data, perhaps using tools such as EOS, AUTOERASE, or

encryption. Sensitive residual data is protected against unauthorized copying and browsing.

IBM has commented on both the ease with which residual data can be abused and the performance improvements that make EOS (AUTOERASE) practical to use. Here's what they say in the "***RACF System Programmer Guide***" (emphasis added):

"*The erase-on-scratch facility provides a defense against two types of attacks:*

1. *It protects against an attempt to read residual data. This means that no one can allocate a new data set at the same location, open it for input, and read your data.* ***This requires no exotic tools or insider knowledge and can be done quite easily using JCL and an IBM-provided utility such as IEBGENER.***

2. *It defends against an attempt to read data by acquiring physical access to a device and attempting to read its data directly." ...*

(And on performance side effects)

"Using data erasure with virtual array devices means that the storage subsystem erases data automatically without performance penalty. DFSMS checks the erase results from the RVA device. If the data was to be erased, DFSMS checks whether it was erased by the device. If it was not, DFSMS erases the data using other methods.

Two general "rules of thumb" flow from this implementation:

1. If you are using the DDSR function of IBM's extended data facility product (IXFP), specifying erase-on-scratch has minimal impact because DDSR performs the erasure in the overwhelming majority of cases.

2. If you have data for which you want to enable erase-on-scratch, allocate the data on DDSR-enabled volumes.

By following these two rules, your data can be erased by the storage subsystem in the overwhelming majority of cases. In those rare cases where the storage subsystem was not able to erase the data, DFSMS erases the data using the ERASE CCW. This is also faster than on older devices because it does not need to wait for disk rotation."

(End of IBM comment)

(Note that the same issue of residual data applies not just to mainframes and not just to disk datasets. It applies to tapes, hard drives on personal computers, and other places where data is stored. If you want to learn what has been copied on a modern photocopy machine, all you have to do is remove the hard drive where it stores the images and pull off the residual data.)

5) Seminar Information and Miscellanea

5A) >>>>Seminar Information

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

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

- How to Audit **z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** May 1-4, 2012 in Raleigh, NC and (November 12-15, 2012 in Clearwater, FL)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (April 11-13, 2012 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

5B >>>>This Issue's Proverb of the Day

"The focus of IS audits should not be whether IT is right or wrong. Rather the focus should be on whether the controls are adequate to support some specified goal (such as supporting the financial audit control objectives)."

5C) >>>>Useful Information

Here's a new source of free, practical information on mainframe security and auditing, from a variety of sources. Topics include:

- Glossary of Mainframe Terms
- How to Get z/OS Basic Skills and IBM z/OS Manuals in pdf Format
- Integrity Statements from CA Technologies and IBM
- z/OS Configuration Info: Documents, Audit Guides from NewEra
- Back Issues of z/Journal Magazine and Mainframe Executive Magazine
- IBM Presentation Handouts on Security and RACF from SHARE and GSE
- Free Articles on Mainframe Security and Auditing

Here's the link: http://www.stuhenderson.com/XINFOTXT.HTM

5D) >>>>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 expand each of these acronyms and explain how the software works in 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

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