MANEWS Issue Number 24

the Mainframe Audit News

This newsletter tells you stuff you need to know to audit IBM mainframe computers running with z/OS and the MVS operating system. This issue we explore resource classes, as well as some of the reasons we continue to experience new breaches all the time. In the next issue in the Fall, we intend to provide coverage of the new releases of z/OS, MVS, RACF, ACF2, and TopSecret.

Table of Contents

1) Structured Mainframe Audit Approach

If you're like many IS auditors, you may feel that you don't have the time, budget, knowledge, and resources to conduct a comprehensive audit. At the same time, you don't like to audit at such a high level that you add little value. A good solution to this dilemma is to break your audit down using structured decomposition.

This breaks the audit approach into pieces which don't overlap, but which add up to a comprehensive audit. You can then address one or more pieces separately, in digestible bites, without losing sight of the big picture. You can also use the breakdown to organize your audit planning, reports, and work papers.

To give an example for mainframe infosec audits, you can break the question “Is our information security adequate?” into these non-overlapping pieces:

1. Can users access the system without being authorized?

2. Can users access data without being authorized?

3. Can users access resources without being authorized?

4. Can users change the security rules without being authorized?

5. Is there adequate separation of duties in security administration?

6. Is the integrity of the MVS operating system maintained?

This next page of this issue of the MANews shows you how to address piece number 3 (resource access). For other pieces, you may want to review earlier issues (please see http://www.stuhenderson.com/Newsletters-Archive.html for back issues)

==========

2) Auditing Resources

On mainframe computers, a resource is anything other than a dataset ("dataset" means the same as "file") that you want to protect. To provide thorough mainframe auditing, you will want to consider where resource protection fits in your audit plan. Whether you use RACF, ACF2, or TopSecret, datasets are protected by dataset rules. And resources are protected by resource rules. Each resource rule is a record contained in the security software database. It lists who is permitted to access the resource.

For RACF and TopSecret, resource rules are organized into standardized resource classes. Each class has a standard class name to describe what it protects. For example the resource class named **OPERCMDS** is used to control who can execute operator commands. The resource rules describing who can issue various operator commands are all "in the OPERCMDS resource class". This just means that they include the word **OPERCMDS** as part of the name of the rule.

ACF2 organizes resource rules into resource types. Most of the types correspond to the standard resource classes used by RACF and TopSecret. For example, ACF2 uses the resource type **OPR** where RACF and TopSecret use the resource class **OPERCMDS**. In ACF2, you can look at the SHOW ALL report to see the names of the standard resource classes and the resource types they get translated to.

On the next page we list some of the standard resource classes which are often considered "essential" for effective security. Note that not all of them are necessarily essential in every installation. Note also that installations sometimes change the names of the classes. However you can learn the new names easily from the audit steps below.

Resource Classes Used By All Three (RACF, ACF2, and TopSecret)

JESSPOOL (to control who can browse other people's printouts)
DASDVOL (to control use of powerful utility programs used for disk maintenance)
UNIXPRIV (privileges in USS, that is UNIX under MVS)
VTAMAPPL (to prevent spoofing of VTAM APPLIDs)
PROGRAM (to control who can execute certain powerful programs)
SERVAUTH (to secure TCP/IP, FTP, TN3270, and more)
PROPCNTL (to prevent propagation of userids for CICS regions)
OPERCMDS (to control who can execute operator commands)
SURROGAT (to control submission of batch jobs with different userids)
WRITER (to control who can route printouts to various printers)
MQADMIN (and related classes, to secure MQ)
DSNR (to control access to DB2)
FSACCESS (to control access to USS file systems)
SDSF (to secure various SDSF functions)

Resource Classes Specific to RACF

FACILITY (essential for so many reasons, we can't list them all here)
TCICSTRN and **GCICSTRN** (for CICS transactions)
NODES (for control of batch jobs and printouts coming in over the network)
APPL (to control access to various CICS and IMS regions, as well as to TSO, USS, and other applids)
GLOBAL (for performance)
TSOAUTH (for TSO privileges)
DIGTCERT and **DIGTRING** (for digital certificates)
RACFVARS (to provide substitution variables for &RACLNDE and others)
STARTED (to assign userids and privileges to started tasks)

Resource Classes Specific to TopSecret

IBMFAC is the name TopSecret uses for what RACF calls **FACILITY** (essential for so many reasons, we can't list them all here)
OTRAN (for online transactions, including CICS and IMS)
VOLUME (for access to datasets and the ability to bypass label processing on tapes)

Resource Types Specific to ACF2

CKC for CICS transactions
FAC is the name ACF2 uses for what RACF calls **FACILITY** and which TopSecret calls **IBMFAC** (essential for so many reasons, we can't list them all here)

To address resource classes in the audit, you'll want to see which of the essential resource classes are in use ("active"). For the active classes, list at least a sample of the rules and determine whether they provide effective protection.

For RACF, see the DSMON Class Descriptor Table Report to determine which classes are active. Use the RLIST command to list a resource rule.

For TopSecret, see the Resource Descriptor Table [output of TSS LIST(RDT) command] to determine which classes are active. Use the TSS WHOHAS and TSS WHOOWNS commands to list resource rules.

For ACF2, see the SHOW ALL report under SAF DEFINITIONSto determine which resource classes are active. See the SHOW ALL report under SAF MAPPING to see how the standard resource class names are translated to ACF2 resource type names. Use the SET RESOURCE and DECOMP commands to list resource rules.

For each essential resource class or type, you will want to verify whether your installation uses it, whether you should be using it, who is the "owner", who approves its rules, what logging is to take place, and how to keep its rules simple enough to be effective while still easy to administer.

There are literally hundreds of resource classes used in mainframe systems. If your audit only looks at userids, passwords, and dataset protection, you will be missing important areas of risk and protection.

The steps listed above give you a starting point to address resource protection in your audits. In future issues we intend to provide more detail about additional steps to evaluate resource protection, as well as additional information describing some of the more important resource classes.

==========

3) Want to Beta Test a New Audit Tool?

A new automated reporting tool is coming to help you address your mainframe's connections to TCP/IP and the Internet. It will give you critical audit information, such as:

- What connections are taking place
- Encryption information about your ports and applications and sensitive data
- Who is probing your network and from what countries

If you would like to know more about this tool, and possibly be part of a beta test program, please contact Stu at stu@stuhenderson.com.

4) Two Very Different Types of Risk

We've seen two very different risk types leading to the infosec breaches we read in the newspapers. One type is **technical**, the result of someone using flaws in the security architecture of the hardware and software to get unauthorized access.

The second, and perhaps more prevalent, type is **people-related**, the result of people not following basic good security practices. Examples include clicking on links in phishing emails, not protecting passwords, leaving vendor supplied default passwords in place, and carelessly leaving sensitive data in unsecured locations. We may never be able to prevent users, IT staff, and other people from failing to follow good practice.

These two types of risk call for different means of mitigation. The technical risks can best be addressed by the hardware and software vendors, and by others with extreme technical knowledge.

The people-related risks may not be preventable. If you accept this premise, then you might find that isolation is the best way to manage the risk. As far as possible, isolate sensitive data on computers separate from most users and networks. If for example, a movie company keeps its movie masters on computers, it makes sense to isolate those computers from the majority of the users and networks.

In short, if you can't force people's behavior, then don't make it possible for most of them to reach the important data. Consider the breaches you've read about in the newspapers so far this year. How many of them would have been less serious if the isolation principle had been better followed?

And of course, mainframes are ideal for implementing isolation, with their lpars, and syplexes, and address spaces and trusted computing bases.

You might ask yourself whether you have included isolation as a possible control in your most recent audits.

5) Where Were the Auditors on the OPM Security Breach?

You may have read about the major infosec breach at the US government Office of Personal Management computers. This is the agency responsible for providing security clearances for government, military, and contractor staff working with sensitive information. Hackers obtained large amounts of sensitive information in this breach, and were not detected for several months. You have to wonder what the agency's auditors were doing to prevent this. The answer is that they had earlier idenitified and documented many significant security weaknesses in the agency's computer systems. They also had provided specific recommendations to improve the security. You then have to wonder how and why and by whom the decision was made not to act on their reports.

This can lead us to ask what effect our audit reports have on our organizations, and whether they result in specific improvements and actual reduction in risk. This can lead us further to some understanding of why we continue to read about new infosec breaches in the newspapers.

The OPM auditors wrote a report so good that we can all benefit by reading it to see how they collected, evaluated, and reported their findings and recommendations. You can read it at:

http://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf

Appendices: Seminar Information and Miscellanea

Appendix A) >>>>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** (September 21-24, 2015 in Chicago)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (November 10-12, 2015 in Bethesda, MD), a logical follow-on to the previous course
- How to Audit **UNIX and Windows Security** (October 26-29, 2015 in Raleigh,NC)

To learn more about them, please go to

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

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

"*Any day I'm upright is a good day.*" — Email tagline

Appendix C) >>>>Useful Information

Two useful sets of guidelines will help you audit more effectively:

- The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes https://web.nvd.nist.gov/view/ncp/repository

- Useful guidelines for knowing that your InfoSec is comprehensive (Note especially Publication 800-53): http://csrc.nist.gov/publications/PubsSPs.html#800-53

An additional source of free, practical information on mainframe security and auditing, from a variety of sources: http://www.stuhenderson.com/XINFOTXT.HTM

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

Appendix D) >>>>About the Mainframe Audit News; 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 for auditors who are new to IBM mainframes, and also for experienced MVS auditors who want to keep up to date with the latest developments. We will not make the list of subscribers available to anyone else for any reason.

To Subscribe or Unsubscribe Click on
http://www.stuhenderson.com/subscribe.html .

To see Back Issues: www.stuhenderson.com/Newsletters-Archive.html

Feel free to contact us at (301) 229-7187 or
stu@stuhenderson.com.