MANEWS Issue Number 28

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 the latest release of z/OS, more steps in your first mainframe audit, and stuff you need to know about encryption..

Table of Contents

1) New Release 2.3 of z/OS System Software

IBM is making a new release (numbered 2.3) of the z/OS system software available September, 2017. This is a major event, since the next release will likely not come until 2021. You probably know already that z/OS is the package of software that includes the MVS operating system, and many related software tools, including TSO, JES, VTAM, and others.

While the basics of z/OS mainframe security are unchanged, the new release:

- Provides new features
- Forces a review of all system software
- Reminds us of dates when software goes off support

New features include:

- New security and tools to make the mainframe be your Cloud
- Policy based encryption of data at rest
- Plans to eliminate a potential exposure involving common storage and the DIAGxx member of parmlib
- A new 119 SMF log record that not only tracks SSL/TLS version but also digital certificate serial number

A review of all the system software will be needed, since each piece of software needs to be tested to make sure it works well with the new z/OS. This is an opportunity to review security for each software product at the same time.

Support dates are the dates when a version of a software product becomes considered obsolete, and no longer automatically supported by the vendor. This usually means that the vendor is no longer committed to fixing bugs in the product. The new release of z/OS is release 2.3. The previous release is 2.2. The ones before that are z/OS 1.13 and z/OS 2.1. The end of support for z/OS 1.13 is September 30, 2016. You can monitor end of support dates for IBM software at http://www.ibm.com/software/support/lifecycle/index_z.html

What This Means for the Audit

The most important new feature is the policy based encryption of data at rest. You will want to get familiar with how it is to be implemented (either by specifying encryption in the dataset rules in the security software or by specifying encryption in the software called System Managed Storage).

One of the first questions for an information system audit is whether management has a reliable inventory of the hardware, software, networks, applications, and data. This is based on the idea that no one can manage something if he doesn't know what it includes.

For security audits on mainframes, a basic step is to evaluate whether management has the controls to know (and to be able to demonstrate) that every privileged program is "safe". "Safe" means that the privileged program cannot be used to break the security of the system.

You may have encountered audits where management states (or you determine) that they do not have an inventory of all the privileged programs on the system, and that they do not have the time and resources to conduct such an inventory.

But when an upgrade to a new release of z/OS is under way, management has to conduct an inventory of all the system software, in order to test it and make sure that it works with the new z/OS. You might suggest before the inventory and testing begin, that this would be an excellent opportunity to develop an inventory of all the privileged programs on the system.

To tell whether the system software is still supported by the vendor, you'll want to get the output of the operator command **DISPLAY IPLINFO**. This will tell you what release of z/OS is running, so you can verify that it is a currently supported release.

2) Three New White Papers on Info Security

These white papers will make you a better security professional:

— Eleven Steps to Make Mainframe Security Audits Better

— What You Need to Know About Bots (Programs that pretend to be thousands of real people posting on FaceBook and Other Sites)

— How to Protect Voting Machines and Registration Data from Hackers

3) Second Steps in Your First Mainframe z/OS Audit

Last issue we discussed how to start your first Mainframe z/OS audit. We described basic data to gather and important scoping considerations. This issue we show you how to continue for a mainframe z/OS operating system audit.

In later issues, we'll show you how to audit:

- Security software (RACF, ACF2, and TopSecret)
- Applications
- USS (the standard UNIX that is part of z/OS)
- TCP/IP on the mainframe.

So what's the point of an operating system security audit? The operating system (think UNIX, Windows, or on the mainframe MVS) provides the foundation for entire security of the rest of the system. It does this by building a virtual cage around each program that is running. This cage prevents the program from touching memory belonging to other programs and from interfering with other programs' execution.

This "cage" is based on hardware controls, which you may safely ignore in your audit. The cage though is the foundation of mainframe security.

It is possible for system programmers to add programs to the system with privileges that let the programs break out of their cage and bypass all the security on the system. There are several ways for system programmers to add such programs, but they all involve updating certain key system datasets.

So your audit will address the controls over who can write to these key datasets. To do this, you will first review the management controls, including policy, procedures, standards, baselines, logging, and monitoring, of the ability to update these datasets. You will then identify these key datasets. Your next step will be to review the dataset rules in the security software dataset to see who has update access to the key datasets. You will note that anyone who can update these key datasets can bypass all the security on the system.

What This Means to the Audit

Collecting and evaluating this data will postition you to determine whether management has the tools to know, and to be able to demonstrate, that all the privileged programs added to the system are:

- Approved, after appropriate analysis and testing
- Protected from unauthorized additions and modification
- “Safe”, that is they don’t introduce security exposures

While this description doesn’t give you everything you need to conduct your first MVS security audit, it does give you a running start. You can learn more from the white papers on our website (described below) and from other issues of this newsletter.

4) European Encryption Regs May Apply to Your Audit

The European Union is implementing new rules called the **GDPR** (General Data Protection Regulation) which may affect your organization in surprising ways. According to the description at http://www.eugdpr.org/gdpr-faqs.html, "the GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location."

What This Means to the Audit

You may want to evaluate the procedures management has in place to ensure that the data center is in compliance with all applicable laws and regulations, including laws protecting sensitive information. You can include audit steps to evaluate how well:

- An inventory of possibly sensitive datasets is maintained
- The Legal, Compliance, and other departments are involved in deciding what regulations apply to which of these datasets
- Tools are implemented to protect this sensitive data. These tools can include encryption, the RACF feature Erase-On-Scratch, and the comparable feature in ACF2 and TopSecret called AUTOERASE.

5) Basic Mainframe Encryption Stuff You Need to Know

On mainframes, to understand encryption, there are two types of hardware, two types of software, and two security software resources classes to be aware of:

The two types of hardware both accelerate processing for encryption and decryption and can therefore greatly reduce hardware and software licensing costs. The first one is free and is called **CPACF** (CP Assist for Cryptographic Function). The second has to be paid for, and is called **CEX** (Crypto Express). In your audit, you will find that without both these hardware features, it will be difficult to provide comprehensive encryption of sensitive data.

The first of two types of software is **ICSF** (Integrated Cryptographic Services Facility), a started task which is a centralized router for requests from programs for encryption and decryption.

The second type of software is called **Policy Agent**, a started task that acts like a firewall for mainframe networks. Policy Agent lets you enforce encryption based policies specified in its configuration files. A policy might specify for example, "***Encrypt all traffic on IP address so and so and port number such and such using this protocol and key***." Having the control centralized means you don't have to modify programs to provide encryption. It also means that you can change keys and protocols easily when requirements change. Both ICSF and Policy Agent are free as part of z/OS.

The two resource classes for RACF, ACF2, and TopSecret are named **CSFKEYS** and **CSFSERV**, and are used by ICSF to control access to encryption keys and to various encryption/decryption functions respectively. Both resource classes are essential to effective security.

You can hear a free recorded webinar on mainframe encryption as well as download the handout that goes with it:

View and hear the recording:
https://newera.adobeconnect.com

Download the handout:
http://www.newera.com/INFO/Crypto_for_CIOs.pdf

Appendices: Seminar Information and Miscellanea

Appendix A) >>>>Seminar Information

Henderson Group seminars are available for in-house as well as public sessions. For more info, please visit www.stuhenderson.com/XAUDTTXT.HTM

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** (February 27-March 2, 2018 in Clearwater, FL)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (November 15-17, 2017 in Bethesda, MD), a logical follow-on to the previous course
- How to Audit **UNIX and Windows Security** (October 24-27, 2017 in Bethesda, MD)

To learn more about them, please go to

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

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

“*Some people have one set of values, other people have others.*”

Appendix C) >>>>Useful Information

Here are more useful information sources to help you audit more effectively:

1. Articles on Mainframe Security
http://www.stuhenderson.com/Articles-Archive.html

New Era offers free webinars by top speakers, and free books to help you audit mainframes better. You can see the seminar schedule and get handouts from previous sessions at
http://www.newera-info.com/The-z-Exchange.html

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

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

4. The current release of z/OS is 2.2. The previous releases are z/OS 1.13 and z/OS 2.1. The end of support for z/OS 1.13 is September 30, 2016. You can monitor end of support dates for IBM software at
http://www.ibm.com/software/support/lifecycle/index_z.html

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

6. IBM z/OS manuals (including Healthchecker under “z/OS System-Level:) http://www-03.ibm.com/systems/z/os/zos/library/bkserv/v2r2pdf/

7. IBM Multi-Factor Authentication Manual http://publibz.boulder.ibm.com/epubs/pdf/azfug100.pdf

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.