MANEWS Issue Number 29

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 take a side trip to explore how to audit mainframe crypto.

Table of Contents

1) How to Audit Mainframe Crypto

The mainframe has special tools to simplify management of encryption and decryption. To show you how to audit their implementation, this section describes: mainframe crypto components, organization essentials for effective crypto, and a series of audit steps.

Mainframe Crypto Components

You need to know about two hardware components and two software components for mainframe cryptography. The two hardware components speed up encryption and decryption processing, avoiding the need to upgrade the power of the CPU.

The first hardware component is free with z hardware systems and is called **CPACF** (CP Assist for Cryptographic Function). It adds instructions to the CPU's hardware instruction set to process encryption and decryption rapidly. It only provides this saving if it is activated and made use of.

The second hardware component is an extra charge item named **CEX** (Crypto Express). It also speeds up CPU processing for crypto functions.

The only risk of not using these two components is that of increased demand (and therefore cost) for CPU power, which could involve increased costs for software licensing.

The three software components are ICSF, Policy Agent, and pervasive encryption.

ICSF (Integrated Cryptologic Services Facility) is a started task that serves as a router for program requests for encryption and decryption. It uses disk datasets to contain the keys used for encryption and decryption. It has its own userid in the security software. It has a configuration file which specifies options such as whether or not to call the security software to control access to keys and use of cryptologic functions. It can invoke the security software (using the **CSFKEYS** and **CSFSERV** resource classes respectively) for these controls. You can learn the names of the ICSF datasets by reviewing its JCL. (**JCL** or Job Control Language is the scripting language for batch jobs and started tasks.)

PAGENT (Policy Agent) is a started task that provides firewall-like capabilities for mainframe TCP/IP, including blocking of ports and centralized enforcement of encryption based on IP address and port number. These options are specified in a series of configuration files which you can identify by reviewing the JCL for PAGENT. You can see the actual settings by reviewing the output of the **pasearch** command.

Pervasive Encryption provides policy based encryption for disk datasets("***data at rest***"), just as PAGENT provides policy based encryption for data in the network ("***data in flight***"). The datasets to be encrypted can be specified in JCL, in the security software, and in the **SMS** (System Managed Software) started task. (SMS is used to provide automatic, centralized control over allocation of disk datasets. It has its own JCL, datasets, and configuration files, which are beyond the scope of this class.)

These tools all provide the means ***to centralize control of encryption on the mainframe***. They will not be used effectively without sufficient support from the organization, including policy, standards, and formal procedures.

Organizational Essentials for Effective Crypto

An IT organization will not have effective encryption of sensitive data unless it has centralized, formal control of encryption. This is because without centralized control, it is impossible to know what data is encrypted and how, in order to stay abreast of changes in technology and in regulations.

If each application makes its own, undocumented decisions about what to encrypt and how, then the CIO (Chief Information Officer) will not be able to demonstrate that all sensitive data is protected and that the organization is in compliance with all regulations.

Effective encryption requires an enforced policy, set by the CIO, that all encryption and decryption of data on any platform is to be coordinated by some designated group (perhaps the same standards group that administers naming standards for datasets and use of TCP/IP ports). It also requires periodic review by the Legal, Compliance, or similar departments of all data to determine what encryption regulations apply to what datasets.

Formal procedures are needed to protect against loss of encryption keys and exposure of encryption keys, and to provide ongoing maintenance of keys.

Reviewing these policy and standard essentials will support your Test of Design for an audit of encryption effectiveness.

Crypto Audit Steps

To audit the effectiveness of a mainframe data center's encryption of sensitive data, follow these steps, stopping at any point necessary to describe risk and recommendations:

1. Obtain copies of relevant: policy, procedures, and standards. Evaluate whether it is clear who is responsible for effective encryption, and that all encryption is to be coordinated by a central group. Determine whether it is clear how information is to flow among: this group, the Legal and Compliance departments, the security software administrators, the standards organization, hardware capacity planners, application developers and application owners. Obtain copy of naming standard for encryption labels and evaluate whether it is followed.

2. Obtain a copy of the inventory of datasets and the determination of which need to be encrypted and how.

3. By interview, determine whether the hardware components CPACF and CEX are used. Inquire what evaluation has been made about most cost-efficient use of them.

4. Review procedures for new applications to determine whether they provide for consideration of encryption requirements.

5. Obtain copies of JCL and configuration files for ICSF and PAGENT. Obtain output of **pasearch** command which lists options in effect for PAGENT.

6. Review security software rules protecting the datasets that ICSF uses to store encryption keys. Review resource rules for CSFKEYS and CSFSERV resource classes. Review approvals and determination process for deciding what these security software rules should specify.

7. For a sample of datasets which are to be encrypted review whether they are encrypted in flight and at rest by evaluating settings in PAGENT and settings for pervasive encryption. Since you are likely not proficient in interpreting these settings, request data center staff to show you where the specification is made to encrypt these datasets. (For example, to use RACF dataset profiles to implement encryption, include the parameter **DATAKEY(CKDS xxx)** where **xxx** is the label of the key as defined in ICSF.)

8. Review procedures for administration and protection of encryption keys. Evaluate risk of keys being lost and of keys being exposed.

9. Summarize the effectiveness of encryption by summarizing associated risks, including risks of: loss of keys, exposure of keys, failure to protect sensitive data, failure to comply with regulations, unnecessary hardware and software licensing costs. Provide practical recommendations as needed.

2) Is the Mainframe Dying?

No. As Bob Thomas notes in "***Enterprise Systems***" (http://enterprisesystemsmedia.com/article/ibm-mainframes-still-the-backbone-of-todays-global-commerce?utm_source=z%2Fflash&utm_medium=newsletter&utm_content=zF+-+art+1&utm_campaign=4mpjm):

"*IBM mainframes are incredibly pervasive in the entire world's global commerce today. It has been referred to as the most powerful transaction processing system of the cloud era, according to Nanalyze (Nanalyze provides objective information about companies involved in disruptive technologies so that investors can make informed investment decisions.)*

Nanalyze went on to say: "IBM mainframes are literally the backbone of today's global commerce handling more than 30 billion transactions a day (more than the number of daily Google searches) including:

- *87 percent of all credit card transactions ($8 trillion a year)*
- *29 billion ATM transactions ($5 billion a day)*
- *4 billion passenger flights a year*
- *68% of the world's production workloads at just 6% of total IT costs*
- *Citi uses IBM mainframes to process 150,000 transactions a second.*
- *The reason why the IBM mainframe remains entrenched in 92 of the top 100 banks in the world is because you just can't compete with them on cost at the moment.*"

Which of course brings us to the question: Are we allocating IS audit resources roughly commensurate with value and importance of computing assets?

3) How to Read JCL

JCL (Job Control Language) is the scripting language for batch jobs and started tasks. It specifies what programs are to be executed and which datasets are to be made available to them. If you want to identify the input and output files for an application, reading the JCL is a good starting point. If you want to identify the configuration file for a started task, again reading the JCL is a good starting point.

JCL statements almost all begin with a double forward slash ('*//*"), followed by a name and a space, and then the statement type. There are three statement types:

- **JOB** which identifies the beginning of a unit of work
- **EXEC** which specifies the name of a program to execute
- **DD** (Data Definition), which defines a dataset (Note: datasets defined as SYSOUT=... are almost always print files. Datasets defined as DD * have their data specified in the immediately following statements. Disk and tape files are identified with the DSN (DSNAME or dataset name) parameter. This name is the name used by the security software to control who can access the dataset.).

See if you can tell which programs are to be executed as part of this batch job, and which datasets are to be made available to them:

```
//JOBNAME1      JOB     USER=PAYROLL,...
//STEP1         EXEC    PGM=PAYEDIT...
//INFILE1       DD      DSN=PROD.PAYROLL.MASTER...
//OUTFILE       DD      DSN=PROD.PAYROLL.NEW...
//EDITFAIL      DD      SYSOUT=A

//STEP2         EXEC    PGM=PAYPRINT...
//INFILE2       DD      DSN=PROD.PAYROLL.NEW...
//CHECKPRT      DD      SYSOUT=B
//PAYCFG        DD      DSN=PROD.PAY.CONFIG.DATA...
```

4) What is SMS (System Managed Storage)?

SMS is software that automatically manages disk datasets. For example, you can use it to specify JCL parameters for a dataset or to specify which group of disk drives a new dataset is to be allocated on. And you can use it to specify what sort of encryption a disk dataset is to have. You do this by means of the DFP segments in the security software. (In order to cause confusion, IBM has named the SMS-related segments of RACF profiles the DFP or Data Facility Product segments.)

SMS allows the DASD storage administrator to define several SMS classes for disk datasets

1. **DATAAPPL** identifies the application such as Payroll or Sales
2. **DATACLAS** specifies predefined JCL values
3. **MGMTCLAS** specifies backup frequency and related values
4. **STORCLAS** specifies I/O service levels for the dataset

Your SMS administrator defines the classes and writes routines to assign them to datasets. You can use DFP segments in the security software to specify the starting point for this assignment. The DFP segments can now be used to specify which datasets are to be encrypted.

5) An Easy Way to Protect Election Computers From Hackers

While this is not a mainframe-specific topic, we expect friends who know you are an IS auditor will ask you about protecting election computers, and what a "bot" is. Here are three useful articles:

For an easy way to protect election computers,
http://www.stuhenderson.com/ProtectVote.pdf

For information on "bots" is and how they can be weaponized,
http://www.ndn.org/sites/default/files/blog_files/NDN-BOTPAPER.pdf

For information on how to recognize a post over the Internet from a "bot",
https://static.politico.com/42/23/98d1424e413898e4fcab56cddbc8/va-gov-bottracker-report-latino-victory-10217.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

To learn more about them, please go to

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

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

"Just go try stuff. If it works for you, stick with it. If it doesn't, then try something else."

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

2. 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

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

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

5. The current release of z/OS is 2.3. The previous releases are z/OS 1.13 and z/OS 2.1 and z/OS 2.2. 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

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

7. IBM z/OS manuals:
https://www-304.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R3Library?OpenDocument

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.