MANEWS Issue Number 16

the Mainframe Audit News

==========

Table of Contents

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

1) What is CICS?

CICS (IBM's Customer Information Control System) is transaction management software that executes on the mainframe. It is one of the most widely used methods for letting people interact with the mainframe from a terminal.

To understand CICS, it helps to contrast it with **TSO** (IBM's Time Sharing Option software that serves as a programmer's workbench). Both CICS and TSO involve users logging on at terminals with a userid and password.

TSO users however can then edit files, print files, compile programs, execute programs, and do anything the **security software** (RACF, ACF2, or TopSecret) lets them do. TSO is designed for programmers developing and testing programs.

CICS is more restrictive. After signing on, a user is permitted to do only certain pre-defined transactions. For example, one transaction might be named **INQ3** (inquiry number 3). It might permit a user to type in a customer number and then have the customer's name and address displayed on the terminal screen. A user of CICS is limited to executing only the predefined transactions which exist on his copy of CICS, and to which he is permitted by the security software.

Whenever a CICS user types in the name of a transaction he wants to execute, CICS can call the security software first, asking "Should I let this user do this transaction?"

This issue we discuss a security audit of the CICS **infrastructure**. Next issue we will cover how to perform a security **audit of a given application** running under CICS. The infrastructure audit addresses the security settings for one copy of the CICS program. These settings determine, among other things, when and whether CICS calls the security software.

Because most of CICS security relies on the security software, we will concentrate this issue on the switches which determine how the security software is used.

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

2) How to Audit CICS: the Infrastructure

Each executing copy of the program which is CICS is called a **region**. It will be either a batch job or a started task. It will therefore have **JCL** (Job Control Language) and a userid (in RACF, ACF2, or TopSecret). It will also have a file containing all its options: the **DFHSIT** or **SIT** (System Initialization Table) (The **DFH** prefix is IBM's abbreviation for CICS.) Each region also has a file called the **DFHCSD** or **CSD** (CICS System Definition) file where all the resources such as transactions are defined.

MANEWS Issue Number 16

the Mainframe Audit News

Planning and Scoping

As you plan and scope your first CICS audit, you will want to find out how many CICS regions (copies) there are in the data center. There may be one for production, one for test, one for Marketing, or one for the Finance application. There may be fifty or more in one data center. Pick one production region where an important online application executes.

To plan your audit, you will want a list of all the regions specifying whether each is test or production or something else, and which applications execute in each region. Note that some regions will be called **TOR**s (Terminal Owning Regions) and some may be called **AOR**s (Application Owning Regions). A TOR is a region used only for sign ons. Once a user signs onto to it, requests for transactions to be executed are shipped from the TOR to the AOR where that transaction's application lives.

To make your first CICS audit reasonably small, try to avoid a region which connects to other regions (TOR/AOR), to DB2, to the Internet, or to MQ Series. These are all complications beyond the scope of this article, but which we hope to address shortly.

For an application audit (described in the next issue), you will want to obtain the names of all the transactions for the application in the region, along with a description of what each one does, and the security software rules describing who can execute which transaction.

But for the infrastructure audit, we will want to see that the region is set up to provide a reliable foundation in which the application's transactions can execute. To do this, we will ask: "*does the security software identify every user and control which users can sign onto the region*" and "*does the security software control which transactions each user is allowed to execute*?". To do that, we'll look at the values in the SIT.

We will show you first the standard approach to securing CICS, and then explain some possible additions if your security software is ACF2 or TopSecret.

In any case CICS can use the security software to answer almost all important security questions:

- "Who is this user?"
- "Can this user come into this region?",
- "Can this user execute this transaction?", and
- "Can this user use this resource (such as a file or destination)?"

Data Gathering

For the region you have chosen, get a copy of the JCL, and a copy of the SIT for your working papers. (The CSD file might be nice, but may be too big for you to get a full copy for now.). From the security software, find out what userid the region executes under, and whether it has any privileges. (It does not need **SPECIAL** nor **OPERATIONS** [in RACF], nor **NON-CNC**L nor **SECURITY** nor **MAINT** [in ACF2], nor **NODSNCHK** nor **NORESCHK** [in TopSecret].)

Note that when a CICS region starts up, it is possible to override some of the operands in the SIT. You can learn about this by reviewing the EXEC statement in the Job Control Language (look for a PARM= operand) and discussing it with the CICS system programmer. You want to be sure that you are looking at the SIT values that the CICS program actually uses, including the overridden values. You should confirm your understanding of this with the CICS system programmer.

Check the following options in the SIT:

SEC= YES or **NO**
XTRAN= **YES** or **NO** or possibly some other value
DFLTUSER=userid
APPLID = applid name (the name that VTAM uses to call this particular region)
STGPROT= **YES** or **NO**

MANEWS Issue Number 16

the Mainframe Audit News

Analyze SIT Operands

If the SIT specifies SEC=YES, this is the starting point to tell CICS to call the security software to answer security questions. **If the SIT specifies SEC=YES, then, CICS will call the security software for all signons.** The security software will be responsible for verifying the userid and password, and for determining whether that user is permitted to sign on to that particular CICS region.

The next question to be addressed is whether the security software is called to control whether a given user is allowed to execute a given transaction, for example INQ3. **If the SIT specifies SEC=YES and also XTRAN= anything other than NO, then CICS calls the security software for every transaction.**

Assuming that this CICS region invokes your security software for each signon and for each transaction, you will then need to evaluate the user definitions and resource rules in the security software. We will show you how in the next issue when we address application auditing.

Note that by convention all the IBM-supplied CICS transactions begin with the letter C. These include the signon transaction (**CESN**) and the system programmers' transaction used to shut down the region (**CEMT**). You may want to treat these separately from the application-specific transactions.

Note the default userid specified in the SIT, for example: **DLFTUSER=GEORGE.** This is the userid CICS uses when no other authenticated userid is available. For example, before someone signs on to the region, he has no established userid. So imagine a user whose terminal is connected to a CICS region, but who hasn't yet entered a userid and password. When that user types in the name of a transaction, such as **INQ3**, or **CEMT**, then CICS calls the security software asking if the userid GEORGE is permitted to that transaction.

One auditor, following the principle of poking around, got his terminal connected to a CICS region and typed in the name of a sensitive transaction without signing on to prove his identity. CICS executed the transaction for him. Researching how this could be, the auditor found that the default userid for that region had been

permitted to that transaction, obviating the need to sign on. This was of course a significant audit finding.

Here are some rules of thumb: Each region should have a unique default userid specified in the SIT. The default userid should be different from the userid of the region itself. The default userid should not have privileges in the security software (such as **OPERATIONS**, **NON-CNCL**, or **NORESCHK)**. The default userid should not be permitted to transactions other than a few harmless ones such as the signon transaction.

So what should you do if you observe a violation of these rules of thumb? Please do not write an audit finding like this: "We noted that the default userid for this region is the same as the userid of the region itself, which we consider wrong. This should be changed."

Subjective opinions which are not risk-based will not survive your closing meeting. Instead, do your homework and identify a risk resulting from failure to follow the rules of thumb: "The default userid has the NON-CNCL privliege in ACF2. This makes it possible for any user of this system to execute sensitive transactions for the xyz application without being authorized, and without having to prove his identity. The xyz application allows users to view credit card numbers which are subject to PCI regulations.". Of course it is always a good idea to link IS audit findings to financial audit control objectives.

Review the APPLID operand in the SIT. This is the name that VTAM uses to call that specific region. So when a user sitting at a terminal wants a connection to a given CICS region, the user specifies the APPLID name in his request to VTAM. The APPLID should be unique to this one region.

The security software uses the APPLID name to decide whether a given user is permitted to sign on to that particular region. Imagine two CICS regions, one for test and the other for production. You want to let programmers sign onto the test region, but only end users to sign onto the production region. Because each region has a unique APPLID, you can use the APPLID value in the security software to separate the two sets of users.

When a user signs on, CICS calls the security software, passing it the userid and password and also the name of the APPLID from the SIT. The security software not only verifies the userid and password. It also checks to see if that user is permitted to that APPLID. In RACF this is done with resource rules in the **APPL resource class**. In ACF2, access to a given region is controlled by bitflags in the LID (user) record.. In TopSecret, the APPLID is translated into a **FACILITY**. You can check the security software rules to determine whether they effectively separate who can sign onto which region.

Depending on what applications execute in the region you are auditing, the use of these rules in the security software may or may not be material.

Note the value of **STGPROT,** for storage protection All of the transactions in a region share the same set of memory (called an "address space"). This means that when two transactions are executing in the region at the same time, each can read and update the other's memory.

If the only transactions in the region are production transactions for the Accounts Payable application, this may not be a problem. If however production Finance transactions execute in the same region as test Marketing transactions, there may be risk that a Marketing transaction could copy or modify Finance data in memory.

You need to review your list of which applications execute in which region. If there appears to be the risk of one application accessing another's data in memory, you will want to look at the value of STGPROT. If it is YES, then the storage protection feature is active. This can prevent one transaction from updating, but not from reading, another transaction's memory. You will then need to discuss with the CICS system programmer which parts of memory are storage-protected, and whether this provides sufficient protection.

In any case, if this risk is there and not mitigated by STGPROT, then you might recommend moving one of the applications to a separate region, in order to isolate it. Note that STGPROT restricts updating of memory, but does not prevent reading of an application's sensitive data by another transaction.

If the installation uses RACF or TopSecret, you will want to check the entry for CICS in the Program Properties Table. In RACF you can see this in the DSMON report titled **PROGRAM PROPERTIES TABLE**. The entry for CICS will have the program name **DFHSIP** (IBM's name for the program which is CICS). A **YES** in either of the other columns indicates that the CICS program has been given privileges beyond what it needs. A **YES** in the column named **"BYPASS PASSWORD PROTECTION**" for the program DFHSIP means that when the CICS program opens a dataset, RACF is not called. This means that the program can access any dataset it wants, regardless of the RACF rules. The risk is that a progarmmer could add a dataset to the JCL for the region, and then modify a transaction to access that file improperly.

In the same report, a value of **YES** in the column "**SYSTEM KEY"** indicates that CICS can acquire all the privlieges of MVS (such as Supervisor State), permitting it to bypass all the security on the system. CICS does not need either of these privleges to function well.

If the installation uses TopSecret, you can get a similar report from the **TSSAUDIT** program, using the **MVS** control statement. The same risks apply.

There is less risk for ACF2 installations, since ACF2 seizes control for the opening of every dataset, regardless of what the Program Properties Table says.

If the installation uses ACF2 or TopSecret, you may need to do further evaluation. Both these products have options which seize control for CICS security, regardless of the settings in the SIT. For ACF2, review the JCL for the CICS region. If it has a DD statement named ACF2PARM, then ACF2 is likely seizing control. You will need to review the options set in the ACF2PARM dataset. These will be similar to the options specified in the SIT, and are described in the ACF2 documentation. Confirm your understanding with the CICS system programmer.

If the installation uses TopSecret, the CICS region may be identified to TopSecret as a FACILITY, which you can verify by listing all the FACILITY rules:

TSS MODIFY (FAC(ALL)) followed by commands to see who is permitted to each CICS FACILITY:

TSS WHOHAS FAC(CICSPROD)

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

Additional Infrastructure Issues

While much of CICS security is covered by evaluating control of signons and transactions, there are additional issues which you may want to include or exclude from your scope. These include:

- **Resource Protection** (for resources other than transactions, like files and destinations)
- **Command Protection** (for control of sub-functions of transactions. For example, to distinguish between the inquire and the shutdown functions of the CEMT command)
- **Userid Propagation** (When a CICS transaction creates JCL and submits it to the system to execute as a batch job, the batch job can inherit the useird of the CICS region, which is likely more power than it needs.)

These considerations are beyond the scope of this article, but can be addressed with the security software. You can learn more by asking the CICS system programmer and the security administrator how they address these. In many cases, addressing just the topics covered in this article will be sufficient for an effective audit.

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

3) New IBM Hardware, So What?

IBM has just come out with a new version of the z series software and hardware. This one is called **z/Enterprise** and it executes on the new **z/196** hardware. We should not consider this just "another hardware upgrade with faster CPU and more memory". This has features which will constitute a revolution in how we configure our enterprise-wide (distributed and mainframe) systems. This will also introduce a new approach to cloud computing. And we will need to learn more buzzwords.

Beyond impressive increases in CPU speed and memory, the z/196 provides a tight connection between the mainframe CPUs and an integrated blade server. A **blade server** is a stripped down collection of circuit boards which act as Windows or UNIX or other system servers. (Each circuit board is one blade. Imagine taking several UNIX and Windows servers from around your organization and putting them all into one box, getting rid of the unneeded keyboards, mice, and monitors. That's a blade server.)

The **zBX**, zEnterprise BladeCenter Extension blade server which comes with the z/196 supports the LINUX, and AIX operating systems. It also includes an x86 processor which could conceivably run Windows or even VMware..

This blade server is tightly integrated by hardware and software with the z/196 mainframe CPU. It comes with the **z/Manager,** Unified Resource Manager to provide workload management and load balancing. The hardware connections provide tightly coupled data paths between the various operating systems, including MVS.

This means that we can replace the combination of a mainframe data center and several server farms with a z/196, supporting all the operating systems in the server farm. The result will be faster data sharing, faster response time, greater flexibility to handle swings in workload, workload sharing, improved security and reliability, and lower costs. The overall cost for electricity and air conditioning will be lower too. And it can all connect easily and securely to the Internet.

This seems to give us all the advantages of cloud computing, without having to transport our sensitive data out of our control to some other company that needs to make a profit off what they charge us.

This also means that auditors will need to know more about how this all works, and how this all affects our audit programs. We intend to provide you more in future issues..

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

4) More on Integrity Statements

We have written in the past about IBM's ***Integrity Statement for MVS***, which gives us assurance that the architecture of MVS prevents any unauthorized program or user from obtaining privileges which let it bypass all the security on the system. We said that as part of an MVS security audit, the auditor should evaluate the tools and methods management uses to know that any purchased software installed on the system maintains the integrity of this architecture (is "safe"). One technique is to request comparable integrity statements from vendors of any software that requires privlieges, statements comparable to IBM's.

CA Technologies (the new name for Computer Associates) provides just such a statement for all their mainframe software, available on their website at: http://arcserve.com/~/media/Files/TechnicalDocuments/common-integrity-statement.pdf .

Now if IBM and CA Technologies both provide this assurance for their privileged software, is there any excuse for any software vendor not to do the same? And if a vendor is not willing to provide such a statement, then how does the system programming manager know that their software is safe? And what effect does this have on the financial audit control objectives? (Note that an integrity statement is not needed for software which does not require privileges such as APF authorization or User Supervisor Calls.)

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

5) Seminar Information and Miscellanea (Useful Articles, Proverb, Interesting Products)

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 **MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (May 9-12, 2011 in Raleigh, NC and then November 7-10, 2011 in Clearwater, FL)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (April 6-8, 2011 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) >>>>Useful Information

If you want to understand the security issues in Cloud Computing, you will want to read NIST's "***Guidelines on Security and Privacy in Public Cloud Computing***". This is their Draft Special Publication 800-144 at

http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

5C) >>>>This Issue's Proverb of the Day

"*Better to do nothing than to waste your time."*

5D) >>>>Interesting Products

While we generally do not recommend or overly criticize software products, we think you will find the following new products of interest:

ESSF, the EKC Security Services Facility, is a new program product to provide enhanced functions for IBM z/OS Resident Security Systems ("RSS"), including RACF..

- Automatically archives profiles as changes are made to the RACF Database(s)
- Password changes by a user may be automatically propagated, even when actual userids are different.
- Instantaneous profile recovery into the active RACF system environment from the ESSF archives at any time.
- Clones Users along with all corresponding accesses, connections, and user dataset profiles.
- Displays, copies Group or User access, connections, and/or profiles.
- Repairs damaged RACF databases.
- Cleans up dormant profiles

Contact Sales@ekcinc.com for more information on EKC Software Products.

==========

Vulnerability Assessment Tool

In our June 2010 newsletter (MANEWS 15), we described a dedicated Systems Programmer who wrote programs which automatically looked for security flaws in priviileged programs by calling them with a variety of different inputs. The result of this work is the Vulnerability Analysis Tool from Key Resources, Inc. and it is now available

on either a license basis or as part of a system integrity vulnerability assessment. For more information, go to www.vatsecurity.com.

==========

ZEN System Event Monitor

captures, views, filters, notifies SyslogD events in real-time, including security violations. Provides triggers for powerful REXX-based automation facilities.

Contact: Graham Storey, William Data Systems, (703) 674 2200, graham.storey@willdata.com, www.willdata.com

==========

Voltage SecureData Encryption Technology

adds controlled encryption technology to existing applications for regulatory compliance, and without key management headaches. Uses the AES Encryption algorithm in an advanced mode known as "Format-Preserving Encryption" (FPE). FPE allows you to encrypt things like credit card numbers or addresses, and the encrypted versions match the format of the originals (n decimal digits, etc.), thus avoiding the need to redo database schema, screens, and the like. Product is multi-platform, with multiple levels of encryption.

Contact: Phil Smith III, phil@voltage.com, www.voltage.com, (703) 476-4511

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

.

5E) >>>>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 will expand each of these acronyms and explain how the software works over the course of 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 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
