Agenda

- Introduction
- Objectives
- Subsystems
- Subsystem Security
  - CICS
  - IMS
  - DB2
  - MQ
  - Others
- Summary
- Questions

IBM Mainframe
Are they really secure?

SPECIALISTS

RSM

Introduction

SPECIALISTS RSM

Introduction

- Mark Wilson
  - Technical Director at RSM Partners
  - I am a mainframe technician who's specialist subject is Mainframe Security
  - I have been doing this for over 30 years (35 to be precise ☺)
  - This is part five of seven one hour long sessions on mainframe security
  - Full details can be seen on the New Era Website:
    - http://www.newera-info.com/MF-SEC.html

SPECIALISTS RSM

My passions outside of work?

- One wife and three daughters…..enough said…..don't have anytime or money for anything else….or so they tell me ☺
- Motorbikes
  - www.wilson-mark.co.uk
- Football
  - www.wba.co.uk
- Scuba Diving
  - Way too many links to list here…..But I have been and dived here
  - http://en.wikipedia.org/wiki/Chuuk_Lagoon

SPECIALISTS RSM

Introduction

SPECIALISTS RSM

OBJECTIVES

Objectives

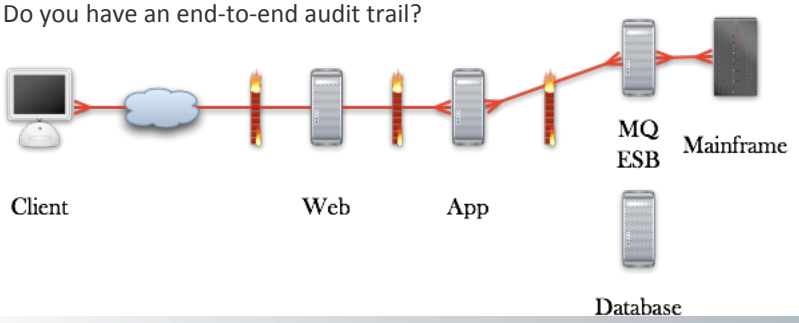
- High level look at some of the many subsystems and the security controls available
- This session is all about subsystem security, subsystems being CICS, IMS, DB2, MQ, etc
- We will then look at the things we need to do, so that we don't have issues with our subsystem security configuration that could be exploited
- We only have an hour and we could spend that just discussing CICS
- Lots of material here for your reference, we wont cover it all, but I urge you all to go away and review how your major applications are all built and secured
- Don't believe what you are told or what is documented…go and check it!!

HOW IT ALL FITS TOGETHER!

SPECIALISTS RSM

How it all fits together!

- A very simple view; looks easy doesn't it?
- But…Do you actually have all of those firewalls in place?
- Is the data that traverses the network encrypted?
- What about Userids & Passwords. How do they flow over the network?
- Do you have an end-to-end audit trail?



SPECIALISTS RSM

SUBSYSTEMS

Subsystems

- We could say where all the real work is done
- CICS; Where the applications run
- DB2 & IMS; Where the data is
- MQ; The data mover
- There are many other subsystems Websphere, JES2, etc
- But we are going to take a high level look at the Application and data ones

Userid Assignment

- All subsystems need a valid user to work correctly
  - RACF Userid controlled via the STARTED Class or ICHRIN03
  - ACF2 LOGONID controlled using the STC privilege
  - TSS User ACID using the *STC* record
- If you can change the userid or UID/GROUP then you could have issues
- Having a Development system running with a Production Userid or vice versa.. Production subsystem running with a Dev. Userid
- The assigned user will need access to many resources:
  - Datasets, FACILITY, FAC, SURROGAT, etc……
  - And resources controlling MQ, DB2, CPSM, etc… as required

SPECIALISTS RSM

What is CICS?

- CICS (UK) or C.I.C.S (USA) or CHIX (The Italians…enough said)
- A transaction processing system, that for some reason has become quite popular over the years!
- Uses Transactions that run programs and the programs access the data
- Used to be able to do internal CICS security….not anymore
- All controlled by your ESM… RACF, ACF2 or TSS
- All of the ESMs work slightly differently in how security is implemented within CICS……..we will use RACF examples going forward
- Not the only transaction processing subsystem that IBM has:
  - IMS & Websphere for instance
- First commercial release July 8th 1969, What happened 13 days later

SPECIALISTS RSM

21st July 1969

The Bible

- CICS Transaction Server for zOS
  - RACF Security Guide
  - SC34-6835
  - This is a CICS publication and not a RACF one
  - Will be found in the CICS Library online or Book Manager
- The CICS Essentials Collection from NewEra has several CICS documents
- They can be found at:
  - www.newera.com

CICS Security

- The CICS 'System Initialisation Table' (SIT) is used by the CICS Systems programmer to specify the desired value for a large number of system parameters used by CICS during initialisation
- The majority of these are internal to CICS itself
- However, there are several system initialisation parameters that CICS provides for specifying the security environment within which CICS will operate
  - Is this a wise thing to do? CICS Sysprogs controlling security parameters??
  - How many sysprogs care about security ☺

SPECIALISTS RSM

The Parameters

- There are many SIT parameters
- The last time I checked there were around 34 security related parameters, but you should check the CICS Security Guide and make your own mind up as which ones are important to you
- The major security ones from my perspective are:
  - SEC=
  - DFLTUSER=
  - SECPRFX=
  - XTRAN=

SPECIALISTS RSM

Security… Yes or No??

- Really is that a question!! Well YES…
- SIT Parameter SEC=
- SEC=NO
  - No External Security Manager being used
- **SEC=YES**
  - External Security Manager is being used
  - This is a mandatory setting in my opinion for ALL CICS systems, even your Test, Development, QA ones

SPECIALISTS RSM

CICS Default User

- SIT Parameter DFLTUSER=
- This parameter sets the userid to be used by the CICS region in a number of "default" situations such as if users are not required to sign on
- If DFLTUSER is not specified it will be set to the value CICSUSER
- The DFLTUSER should always have no or very low levels of access to the CICS region
- You should regularly check which resources all of your default CICS users have access to

SPECIALISTS RSM

CICS Transaction Security

- CICS can apply two levels of security to transactions
  - The first is security checking on the transaction itself, sometimes referred to as attach-time, or transaction-attach security, the security checks that CICS performs to verify that a terminal user is authorised for the transaction to be run at the user's terminal
  - Transaction-attach security applies to transactions that a user enters directly at a terminal, and also to transactions started from another CICS transaction
  - The other level of security you can use for CICS transactions applies to the resources used by the transactions i.e. files, databases, PSBs, and CICS commands

CICS Transaction Security

- Category 1 transactions
  - Never associated with a terminal, they are for CICS internal use only, and should not be invoked from a user terminal
  - CICS checks that the region userid has the authority to attach these transactions, transactions such as CATA, CATD, CDBD, CDBF, CDBO, etc
- Category 2 transactions
  - Initiated by the terminal user, or are associated with a terminal
  - Restrict access to initiate these transactions to userids belonging to specific RACF groups
  - Usually for system programmer use only
  - Transactions such as CDBC, CEDA, CEMT, CESD, CETR, CIND, etc

CICS Transaction Security

- Category 3 transactions
  - Initiated by the terminal user or associated with a terminal
  - All CICS terminal users, whether they are signed on or not, require access to transactions in this category
  - For this reason, category 3 transactions are exempt from any security check, and CICS permits any terminal user to initiate these transactions
  - Transactions such as CLR2, CLS1, CLS2, etc

CICS Transaction Security

- Apart from the IBM supplied transactions you may have ISV software that is used under CICS
- But you will definitely have your own business transactions that execute your own application programs
- You need to protect these transactions as you would any other business resource
- Least privilege is the way to go and hopefully using RACF groups on a Role Based Access Control security model
- Review who has access on a regular basis
- Don't forget to understand the business requirements for Separation Of Duties (SOD)

CICS Transaction Security

- SIT Parameter XTRAN=
- For Production systems transaction security is mandatory
- There are 3 possible values associated with this parameter
- **YES**
  - CICS calls RACF, using the default CICS resource class name of TCICSTRN, to verify that the userid associated with a transaction is authorised to access the transaction
  - Resources defined in the RACF grouping class GCICSTRN could have been used to build the actual RACF profiles used for authorisation checking

CICS Transaction Security

- **name**
  - CICS uses the Tname and Gname user defined resource class profiles for transaction attach security checking
  - The value has a maximum length of 7 characters
  - Using different resource classes is an alternate approach, which can also be used in conjunction with profile prefixing (SECPRFX)
- **NO**
  - CICS does not call RACF to check transaction attach security
  - As transaction security is mandatory for Production, this value should never be used

Profile Prefixing

- SIT Parameter SECPRFX=
- This parameter is extremely helpful if the installation is running multiple CICS regions with differing security requirements and you don't want to use separate RACF classes
- You use the SECPRFX system initialisation parameter to specify whether you want CICS to prefix the resource name RACF checks to allow you to segregate access

Profile Prefixing

- There are 3 options on the SECPRFX parameter:
  - YES
    - CICS prefixes all resource names with the CICS region userid when talking to RACF.
  - NO
    - CICS doesn't prefix resource names in requests it passes to RACF from this region.
  - prefix
    - CICS prefixes the resource names with the specified prefix when passing authorization requests to RACF

CICS Applid Security

- The gateway to your applications/CICS Systems
- Controlled via a RACF class APPL
- Users need READ access to this to be able to logon to the application
- The resource checked is the VTAM APPLid as defined in the CICS start-up parameters
- Before we made life easy users would enter
  - LOGON APPLID(PRDCICS)
  - PRDCICS being the application and therefore the resource checked in the APPL class

SPECIALISTS RSM

CICS Inter Region Communications

- The CICS system programmer is responsible for defining the parameters for cross CICS region communication in the CSD CONNECTION definition, there is no SIT parameter for this
- The CICS ATTACHSEC operand specifies the signon requirements for incoming transaction attach requests
- It has no effect on attach requests that are issued by your system to a remote system

SPECIALISTS RSM

ATTACHSEC

- ATTACHSEC = local
  - Specify if you do not want to make a further check on users by requiring a user identifier or password to be sent
  - If one is received, the attach fails
  - Choose LOCAL if you do not want user security because you consider that the authority of the link is sufficient for your system
  - CICS makes the user security profile equivalent to the link security profile
  - You do not need to specify RACF profiles for the remote users
  - LOCAL is the default value.

ATTACHSEC

- ATTACHSEC = identify
  - Specifies that a user identifier is expected on every attach request and all remote users of a system must be identified to RACF
  - For MRO connections, if an attach request with both a user identifier and a password is received on a link with ATTACHSEC(IDENTIFY), CICS rejects the attach request

ATTACHSEC

- ATTACHSEC = verify (LU6.2 only)
  - If a userid and an invalid password, or a userid and no password is received for verification, the attach will be rejected
  - If no userid is received, CICS applies the security capabilities of the default user.

ATTACHSEC…. Summary

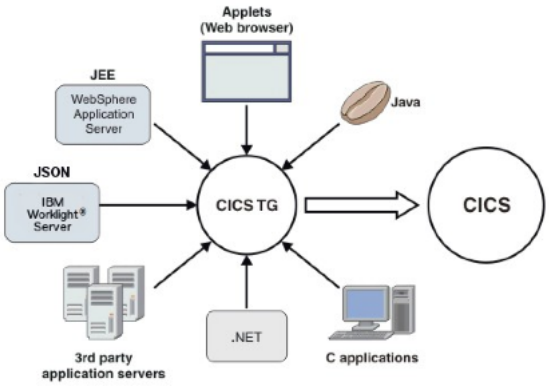
- In an LU6.2 or MRO environment, two basic security requirements must be met before a transaction can be initiated:
  - The link must have sufficient authority to initiate the transaction.
  - If anything other than ATTACHSEC(LOCAL) has been specified, user security is in force. The "user" who is making the request must therefore have sufficient authority to access the system and to initiate the transaction

CPSM

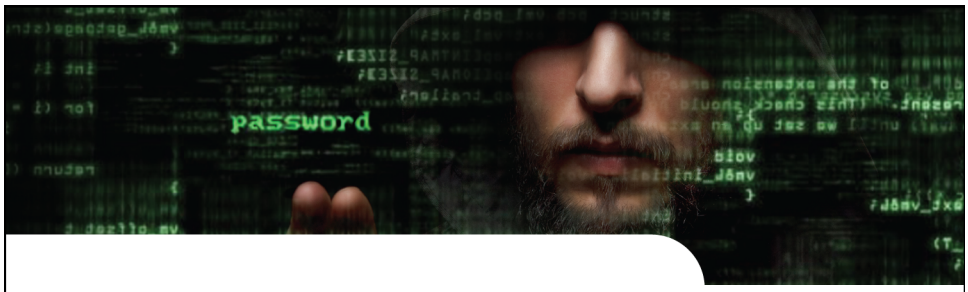
- CICSPlex System Manager (CPSM) provides a central point of control when running multiple CICS systems
- The application uses IBM supplied RACF General Resource class CPSMOBJ to determine operational controls within a CICS complex
- IBM also provides RACF General Resource class CPSMXMP
- Resources in this class can be used by CICSPlex System Manager to identify exemptions from security controls within a CICS complex
- Not widely used, but if you site uses it you need to check the resources defined and who has access and why

SPECIALISTS RSM

CTG – CICS Transaction Gateway



SPECIALISTS RSM



IMS

SPECIALISTS

RSM

IMS

- Information Management System
- A sophisticated Transaction and Database manager
- Which delivers consistently high levels of:
  - Performance
  - Security
  - Scalability
  - Availability

SPECIALISTS

RSM

IMS Security

- Access to IMS resources can be secured by either IMS itself or by an external security product
- IMS provided a basic level of protection using internal facilities such as SMU and/or Security exit routines
- SMU was removed from IMS at V10
- Today an ESM (RACF, ACF2 or TSS) is the most commonly used method of protection
- Advantages of an ESM over IMS Security:
  - One product protecting resources for multiple subsystems like CICS and DB2
  - All resource security information resides in the ESM rather then being distributed among subsystems
- An ESM can offer features such as user identification (USERID) and access verification not available via IMS Security SMU

SPECIALISTS RSM

SECURITY MACRO

- The SECURITY macro specifies the IMS security options to your ESM, such as RACF, the SMU, and IMS Security Exit routines

```
SECURITY TYPE=RASRACF,
RCLASS=IMS,
SECCNTL=2,
PASSWD=YES,
TRANCMD=YES
EJECT
```

- With the release of IMS V13 the SECURITY macro has become obsolete and removed from the SYSDEF procedure
- The security options that were coded in the SECURITY macro are now coded within DFSPBxx and DFSDCxxx PROCLIB members using the following initialisation parameters ISIS, RCLASS, RCF, SECCNT, SGN, and TRN

SPECIALISTS RSM

IMS Resource Protection

- **IMS Commands** should be secured by your ESM, such as RACF (CIMS/DIMS classes), and/or DFSCCMD0 exit routine
- **IMS transactions** should be secured by your ESM, such as RACF (TIMS class), and/or DFSCTRN0 exit routine
- To perform transaction authorization, the SECURITY macro should be coded to specify: SECLVL=TRANAUTH,SIGNON
- **IMS databases** should be protected by your ESM, such as RACF or during the PSB generation (PSBGEN) process

SPECIALISTS RSM

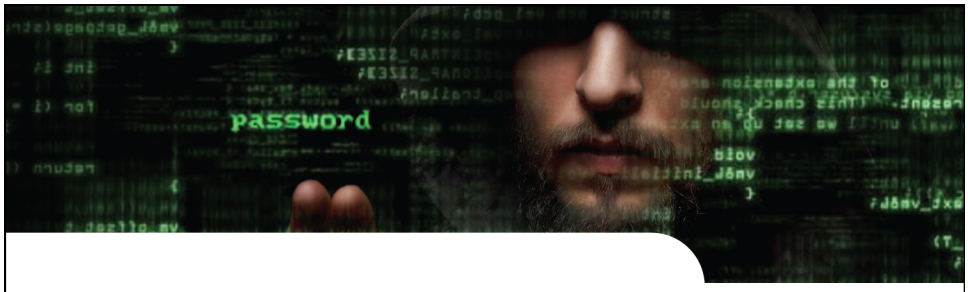
IMS Resource Protection

- **IMS data sets** should be secured using your ESM, such as RACF (PIMS/QIMS, SIMS/UIMS, FIMS/HIMS, and OIMS/WIMS classes)
- **IMS dependent regions** should be protected using Application Group Name (AGN) security
  - AGN security:
    - Protects a PSB by only allowing the PSB to be scheduled by dependent regions that are authorised to schedule it
    - Protects an dependent region by allowing the dependent region to only schedule work it is supposed to schedule

SPECIALISTS RSM

IMS Resource Protection

- A security profile within your ESM, such as the RACF AIMS class should correspond with AGN group name and specify USERID's and/or groups that are authorised
- If an ESM such as RACF is not used then the Resource Access Security Exit routine (DFSISIS0) can be customised for use
- Another feature of IMS is Encryption of data in a file or data being transported over a network. Along with other external tools IMS provides the IMS Segment Edit/Compression exit routine to carry out Encryption



DB2

DB2

- DB2 is a set of database products from IBM
- Originally they supported a relational model, but in recent years some products have been extended to support object relational features and non-relational structures like JSON and XML
- Originally there was a DB2 for each of IBM's major operating systems
- However, in the 1990s IBM produced a DB2 "common server" product, designed with a common code base to run on different platforms
- So, today you get DB2 for Linux, Unix and Windows (LUW) as well as z/OS

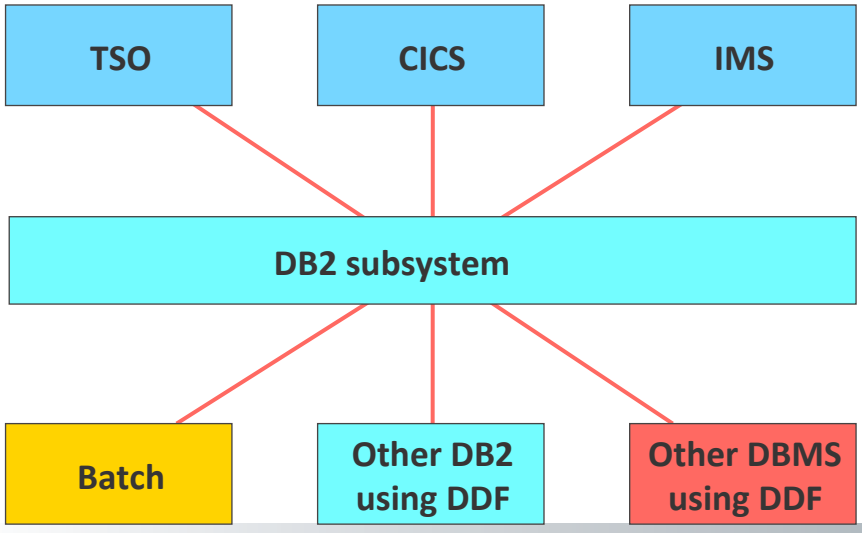
DB2

- DB2 Security can be configured to be:
  - Internal using a series DB2 tables prefixed SYSIBM.SYS*
  - Or externally using the DB2 security exit (DSNX@XAC)
- Whilst external security has been around for while, the majority of sites still use internal security
- So to be able to audit DB2 internal security you need to dust of your SQL skills or find a friendly Developer or DBA who can generate the reports you need
- A good start for all things Security related for DB2 is the IBM Redbook
  - Security Functions of IBM DB2 10 for z/OS, September 2011
  - http://www.redbooks.ibm.com/redbooks/pdfs/sg247959.pdf

External Security for DB2

- You can use an ESM, such as RACF to protect your DB2 resources
- Whilst you can use ACF2 and TSS for DB2 security we will look at RACF
- There are three functional areas to consider regarding protection for DB2:
  - DSNR RACF class
    - The RACF DSNR class controls access to the DB2 subsystems
  - Secondary authorization IDs
    - DB2 identification and signon exits (DSN3@ATH and DSN3@SGN) are used to assign authorisation userids
  - Grant statements/Resource Access
    - There are several RACF classes that depending on what a user is trying to access will need to be granted

The DSNR Class



The DSNR Class

- Profile name has the form ssid.environment where:
  - ssid is the 1 to 4 character DB2 subsystem name
    - For example DSN1 or DB2T
  - Environment may take the value:
    - MASS - Multiple Address Space Subsystem
    - SASS - Single Address Space Subsystem
    - BATCH - Batch Environment
    - DIST - Distributed Data Facility
    - RRSAF - Recoverable Resource Manager Services A/F

Security Exit

- Called at three points
  - At start-up
    - Loads profiles for RACF/DB2 authorisation checking into data spaces (Globally RACLISTed)
  - During DB2 use
    - Check user's authority to specific resources
  - At shut-down
    - Clean up profiles loaded into data spaces
- Supplied in source code format so that site specific options can be chosen
- One of the choices to be made is…….

Multi or Single…Your decision!

- **Multi-subsystem scope**
- The default
- One set of resource classes can protect multiple subsystems
- General resource names prefixed with DB2 subsystem name
- Classes provided in IBM supplied CDT are multi-subsystem scope
- Protect multiple subsystems with single set of resource profiles
- Fewer classes overall

- **Single subsystem scope**
- Optional
- One set of resource classes dedicated to a single subsystem
- General resource names are not prefixed with DB2 subsystem name
- Classes must be defined by the installation
- Segregate resources by subsystem
- Fewer profiles per class

SPECIALISTS RSM

DB2 to RACF Mapping

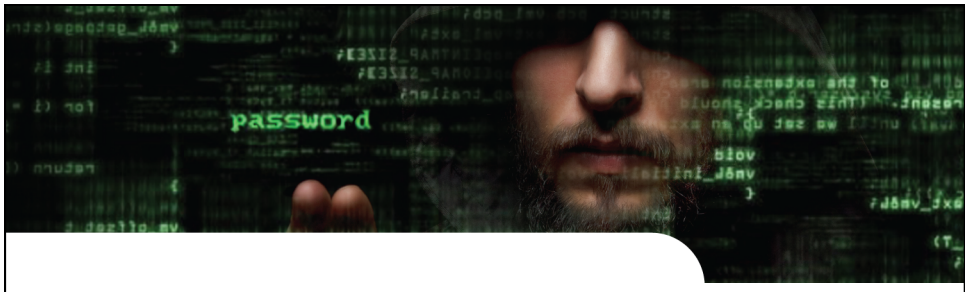
DB2 Object Type	RACF Class Name
DB2 Subsystems	DSNR
Bufferpool	MDSNBP / GDSNBP
Collection	MDSNCL / GDSNCL
Database	MDSNDB / GDSNDB
Package	MDSNPK / GDSNPK
Plan	MDSNPN / GDSNPN
Schema	MDSNSC / GDSNSC
Sequence	MDSNSQ / GDSNSQ
Storage Group	MDSNSG / GDSNSG
Stored Procedure	MDSNSP / GDSNSP
System	MDSNSM / GDSNSM
Table / Index / View	MDSNTB / GDSNTB
Tablespace	MDSNTS / GDSNTS
User Defined Distinct Type	MDSNUT / GDSNUT
User Defined Function	MDSNUF / GDSNUF
Administrative Class	DSNADM

SPECIALISTS RSM

DB2: What to check

- You need to go and look at the profiles in each of the RACF classes used
- Either the IBM supplied ones or the ones you have defined yourself
- Normal rules apply:
  - What is the UAC?
  - What Users/Groups on the ACL and what access to they have?
  - What are the audit settings?
  - Is the UACC and AUDIT settings what your security policy and business require
  - Who has access?
  - Is it appropriate?
  - What about Segregation of Duty?

SPECIALISTS RSM



MQ

SPECIALISTS RSM

MQ

- We will have to save this for another day
- This slide 55 and we only have an hour…
- Will look to do another session on MQ security in the near future
- As I said at the start we could discuss each one of these topics for an hour…

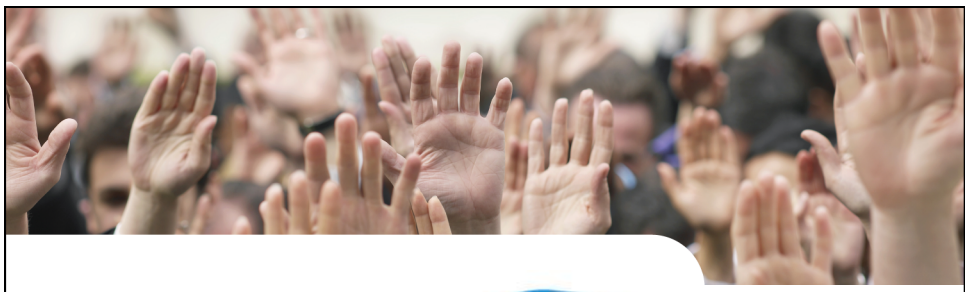
Others

- Don't forget
  - Websphere aka WAS
- What about the others
  - Adabas & Natural
  - CINCOM, Mantis and SUPRA
  - GENEROL
  - To name but a few……

Summary

- You need to be well informed about the end to end security configuration of your applications, especially any of those that may be internet facing
- If you don't understand it how can you be certain its secure!
- You need the knowledge and then YOU must test them or get them tested
- Because today its not a case of if the bad guys are in your network and looking at your applications!!!
- They are here …. we need to understand what can we do to stop them hurting us

SPECIALISTS RSM



Questions

SPECIALISTS RSM

Contact

Mark Wilson
RSM Partners
eMail: markw@rsmpartners.com

Mobile: +44 (0) 7768 617006

www.rsmpartners.com

SPECIALISTS

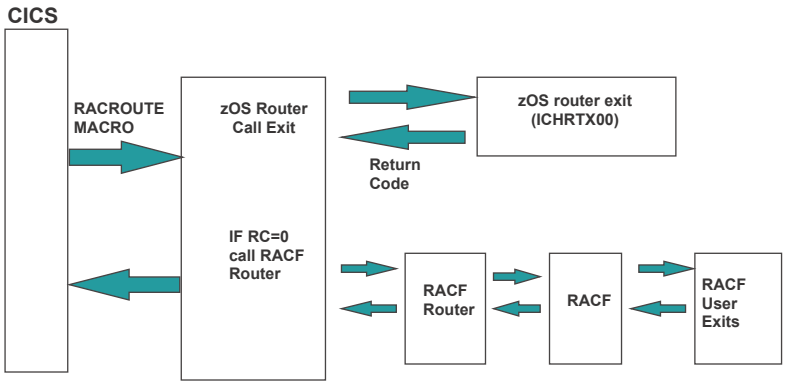
RSM

Additional CICS Slides from an Audit perspective

SPECIALISTS

RSM

The CICS RACF Interface



The role of CICS in security control

- To invoke SAF via RACROUTE to perform:
  - User Signon/Signoff
  - Access Authorisation
- To permit or deny access to protected resources
  – Not RACF!!

Region-wide requirements

- Region must identified to RACF
- The CICS Region Userid
  - Must have correct level of access to:
    - Data set resources (System & User)
    - VTAM resources (ACB)
    - Log Streams
    - Temporary Storage
    - JES Resources
    - Coupling Facility resources
    - Key Rings

Region-wide requirements

- Each CICS Region has a default Userid
  - Specified by DFLTUSER= in CICS SIT Parameters
  - If this is omitted the default is CICSUSER
- Used when no other Userid is present
- Should have very limited access to resources
- This is one of the things to check, what does the default Userid have access to?

User Requirements

- Valid Userid & Password to be able to logon to the CICS region
- Access to VTAM APPLID if protected
- Access to all required CICS transactions if protected
- Access to any other resources that are protected by RACF

What to review?

It depends!

- The biggest constraint we have when auditing a system CICS or otherwise is time!
- If we have enough time we should Audit all aspects of the CICS configuration

What do we need to know?

- What have you got?
- What CICS parameters are you using?
- Is RACF being used?
- What RACF resources are being used?
- What RACF profiles do I have?
- Who has access to them?
- How are the CICS datasets protected?
- Who has access to them?

What have you got?

- This is sometimes the most difficult part as it means interaction with the system programming team ☺
- You need to ascertain how many CICS regions you have and the location of the JCL used to start each of them

What have you got?

- Document all CICS regions and decide which ones to audit
- All of them if you have time; but how often does that happen
- Typically we would do Production first!
- Followed by:
  - Pre-Production/QA/etc…..
  - Development
  - Test – Very rarely audited

What CICS parameters are you using?

- You need to review the CICS startup parameters and determine the SIT parameters in use
  - SIT = Systems Initialisation Table
- The SIT parameters can be in two forms:
  - LOAD Module created with typical settings
  - Override parameters passed at CICS startup
- It's easier to ask the System Programmer what is being used

SPECIALISTS RSM

Sample SIT Parms

```
APPLID=(CICSTS32,CICSTS32),
CICSSVC=216,
FCT=NO,
GMTEXT='RSM CICS/TS 3.2 SYSTEM',
GRPLIST=(XYZLIST,CICSTS32),
IRCSTRT=YES,
ISC=YES,
STATRCD=ON,
SEC=NO,
TCT=NO,
TRTABSZ=64,
XRF=NO,
.END
```

So what's the problem with these parameters?

Hint: Something to do with Security

SPECIALISTS RSM

Is security being used?

- SEC=NO
  - No External Security Manager being used
- SEC=YES
  - External Security Manager is being used

SPECIALISTS RSM

What is being protected?

- Controlled by several other parameters in sit in the form Xnnnn=
- Where:
  - XTRAN = Transaction Security
  - XFCT = File Control Security
  - XCMD = Command Security
  - XTST = CICS Temp. storage control
  - XPCT = Started Transaction control
  - To name but a few!

SPECIALISTS RSM

Xnnn SIT Parameters

- The majority of the Xnnn SIT parameters follow the form:
  - **NO**
    - Option is disabled
  - **YES**
    - Option is enabled with default IBM RACF classes
  - **Class_name**
    - The installation has created a site specific RACF class, normally a pair member & grouping

CICS Transaction Security

XTRAN SIT Parameter

- If XTRAN=YES
  - then the IBM supplied RACF classes TCICSTRN & GCICSTRN are being used for transaction security
- If XTRAN=£PRDTRN
  - then the site defined RACF classes T£PRDTRN & G£PRDTRN RACF classes are being used for transaction security
  - Note that CICS enforces the first character of the RACF class for transaction profiles to be a T
  - Other resource types have their own rules

SPECIALISTS RSM

What RACF profiles do I have?

- Use the RACF SEARCH command to list all of the profiles in a given class:

```
SR CLASS(TCICSTRN) NOMASK
SR CLASS(GCICSTRN) NOMASK
```

- This only shows the profiles
- Or use you're a RACF Administration Tool Vanguard, zSecure, etc, to list the profiles if available

SPECIALISTS RSM

Who has access to them?

- You need to list each profile and check:
  - UACC
  - Access List
  - Conditional Access List
- You can generate the required RACF commands with the SEARCH command and CLIST option
- Or use you're a RACF Administration Tool Vanguard, zSecure, etc, if available

SPECIALISTS RSM

Example Search in batch

```
//SEARCH EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
 SR CLASS(TCICSTRN) NOMASK NOLIST -
  CLIST('RL TCICSTRN ' ' ALL')
//*
//EXEC   EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
 EX EXEC.RACF.CLIST
```

SPECIALISTS RSM

CICS Transaction Security

- Typically the primary focus of most CICS audits
- IBM supply many transactions as part of the basic CICS install
- They are categorised as:
  - Category 1
  - Category 2
  - Category 3

Category 1

- CICS Internal use only
- Never associated with a terminal
- CICS region Userid needs READ access
- All RACF profiles should have a UACC of NONE

Category 2

- CICS Administration transactions
- Very powerful
- Very restricted access lists
- All RACF profiles should have a UACC of NONE
- May be a good candidate for AUDIT(ALL(READ)) to log all access successful or not

Category 3

- All users require access to these transactions
- All Category 3 transactions are exempt from security checks
- It's a good idea to define them to RACF for documentation purposes
- UACC of NONE
- With an * READ on the access list

Business Transactions

- You need to review the access requirements for your own transactions based on the functionality they provide
- There is no one-size-fits-all RACF profile
- Just use basic security principles:
  - Only grant access if required for genuine business reasons
  - Log access to sensitive business transactions
  - Ensure separation of duties
  - Use role based access if available

SPECIALISTS RSM

Member or Grouping Class

SPECIALISTS RSM

Member or Grouping Class?

- Do we have member of grouping class profiles?
- How does CICS use them?
  - Profile merge
  - In Storage profiles
- Who has access?

SPECIALISTS RSM

Example of Member Class Profiles

- The warehouse group of users needs access to three transactions: INVC, ORDP & STOH

```
RDEFINE  TCICSTRN  INVC  OWNER(SECADM)  UACC(NONE)
RDEFINE  TCICSTRN  ORDP  OWNER(SECADM)  UACC(NONE)
RDEFINE  TCICSTRN  STOH  OWNER(SECADM)  UACC(NONE)

PERMIT  INVC  CLASS(TCICSTRN)  ID(WHSEUSRS)  ACCESS(READ)
PERMIT  ORDP  CLASS(TCICSTRN)  ID(WHSEUSRS)  ACCESS(READ)
PERMIT  STOH  CLASS(TCICSTRN)  ID(WHSEUSRS)  ACCESS(READ)
```

SPECIALISTS RSM

Example Grouping Class Profiles

- The warehouse group of users needs access to three transactions: INVC, ORDP & STOH

```
RDEFINE  GCICSTRN  WARE_TRNS  OWNER(SECADM)  UACC(NONE)
RALTER  GCICSTRN  WARE_TRNS  ADDMEM(INVC  ORDP  STOH)

PERMIT WARE_TRNS CLASS(GCICSTRN) ID(WHSEUSRS) ACCESS(READ)
```

SPECIALISTS RSM

How RACF merges Profiles

- Member / grouping classes must be loaded into memory
- Applies only to member / grouping classes
- Merge applies only if a resource name appears in more than one profile
- UACC
  - the most restrictive UACC is chosen from the profiles that are merged
- Access list
  - if a user or group appears in the access lists of multiple profiles, that user or group is given the highest access

SPECIALISTS RSM

Who has access to STOH?

- We must find and analyse all member and grouping profiles that protect STOH
- Is STOH protected by a member class profile?

```
RLIST  TCICSTRN  STOH  AUTH
```

SPECIALISTS RSM

Who has access to STOH?

- Is STOH protected by a grouping class profile(s)?

```
RLIST  TCICSTRN  STOH  RESGROUP
```

- Use RLIST to display any grouping class profiles identified
- Analyse all profiles that protect STOH
- You need to factor this into the Audit and fully understand what you have

SPECIALISTS RSM

CICS Dataset Security

SPECIALISTS RSM

How are my CICS datasets protected?

- You need to document all of the datasets referenced in your CICS startup JCL
- Pay particular attention to datasets that are:
  - APF Authorised
  - Contain SIT override parameters

SPECIALISTS RSM

Who has access to them?

- List the RACF dataset profile that protects each CICS dataset and check:
  - UACC
  - Access List
  - Conditional Access List
  - Warning
- Review any inappropriate settings and amend as required

SPECIALISTS RSM

Who has access to them?

- A RACF command of the form detailed below will show the RACF dataset profile protecting a particular dataset:

```
LD DA('cics-dsn') ALL GENERIC
```

- You need to determine the RACF dataset profile for all CICS related datasets

SPECIALISTS RSM