Cost-effective Automated Mainframe Security

Mark Wilson
RSM Partners

3rd March 2011
Session Number: **8589**

SHARE
in Anaheim
2011

Agenda

Introduction

- I am a mainframe technician with some knowledge of RACF
- I have been doing this for almost 30 years
- This session will look at how to automate system z security functions using zSecure
- Happy to take questions as we go

Language!

- And I don't mean bad language!
- Two countries separated by a common language!
- When is a ZEE not a ZEE?
- When it's a ZED
- What is PARMLIB(e)?
- When its PARMLIB

What's this?

- Zeebra?
- No it's a Zebra!
- Hopefully this will help you understand me ☺

Cost Effective Automated Mainframe Security

So what's it all about?

So what's it all about?

- Because of its reputation for providing the most secure platform in the enterprise, many organizations run their mission-critical applications and centralise their data on mainframes

- It can be a challenge dealing with the complexity and scope of provisioning users, controlling resource access, auditing event and compliance reporting

- Cost-effective security can be achieved with simplified administration, consistent security policy enforcement, state-of-the-art event analysis and automated audit and compliance reporting

- Effective mainframe security can help you reduce costs, improve service and manage risk in your enterprise

Some of the things we need to do?

- Verify the protection of the Trusted Computing Base
  - Identify exposures, document your parameters to the auditors
- Know your privileged users
  - No excessive privileges, unneeded access
- Limit authorities and data access to current job roles
  - Remove unneeded and obsolete authorities
- Remove inactive user ids
- Remove inconsistencies, redundant entries
- Remove superfluous access rights

What's Automation

- Scheduled processes for regular tasks

- Automatically enforcing policy

- Automating manual processes

Scheduled Automation

■ We can schedule regular batch processes to:

  ■ Automation of regular Audit functions

  ■ Perform Status Audit

  ■ Perform compare against baseline

Automatic Enforcement

- Provide automation to enforce the agreed security policy

    - Enforce policy for all RACF commands issued
        - Deny command
        - Correct command

    - Automatically react to events as they happen
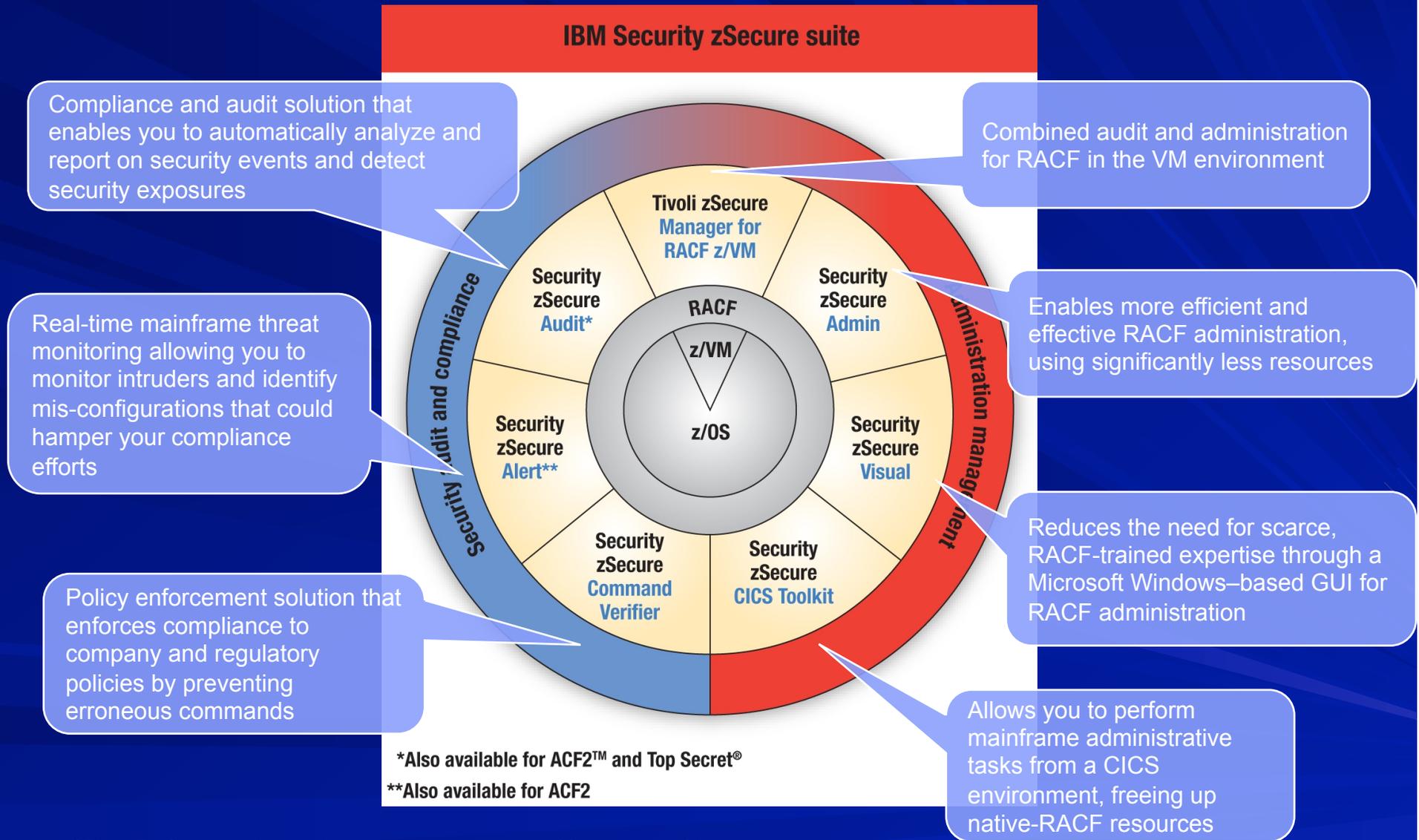
Automating Manual Processes

- Automate the generation of RACF commands when:
  - Creating, Modifying, Listing & Deleting RACF Profiles:
    - Users
    - Groups
    - Datasets
    - General Resources
  - Performing housekeeping tasks such as mass cleanup of a RACF database

Cost Effective Automated Mainframe Security

So how could we do it?

IBM Tivoli zSecure Suite

IBM Security zSecure suite

Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

Combined audit and administration for RACF in the VM environment

Real-time mainframe threat monitoring allowing you to monitor intruders and identify mis-configurations that could hamper your compliance efforts

Enables more efficient and effective RACF administration, using significantly less resources

Policy enforcement solution that enforces compliance to company and regulatory policies by preventing erroneous commands

Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

Security audit and compliance

Administration management

Tivoli zSecure **Manager for RACF z/VM**

Security zSecure **Audit***

Security zSecure **Admin**

RACF

z/VM

z/OS

Security zSecure **Alert****

Security zSecure **Visual**

Security zSecure **Command Verifier**

Security zSecure **CICS Toolkit**

***Also available for ACF2™ and Top Secret®**

****Also available for ACF2**

Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

Cost Effective Automated Mainframe Security

Scheduled Automation

Automation of regular Audit functions

Regular Audits

- zSecure Audit standard reports

  - Many standard audit reports readily available

  - Others can be composed via the standard panels

  - Finally, build your own reports with CARLa

zOS Status Audit – Detailed Reports

```
Session A - [32 x 80]                                                      □ ☐ ☒
 zSecure Admin+Audit for RACF Display Selection            Line 1 of 109

    Name        Summary Records  Title
 _  SYSTEM           1       1  System settings and software levels
 _  SYSTEMAU         1       3  System settings - audit concerns
 _  IPLPARM          1       1  Effective system IPL parameters
 _  SMFSUBOP         1       6  SMF subsystem-dependent settings
 _  SUBSYS           1     108  Subsystem Communication Vector Tables
 _  VSM              1      21  Virtual storage map
 _  WRITABLE         1       7  Globally Writable Common Storage
 _  MPFMSG           1      23  Message Processing Facility message intercepts
 _  JOBCLASS         1      36  JES2 Job Class parameters (e.g. MVS command auth / B
 _  CONSOLE          1      71  Operator Consoles
 _  PPT              1     101  Program Property Table
 _  SVC              1     160  Supervisor Call Audit Display
 _  PC               2    1054  Program Call Audit Display
 _  TAPE             1       1  Tape protection settings (RACF)
 _  IOAPP            0       0  Authorized I/O Appendage table
 _  DMS              0       0  DMS system settings
 _  DMSAUDIT         0       0  DMS system settings - audit concerns
 _  EXITS            1      59  Exit and table overview
 _  DASDVOL        163     163  DASD Volume Protection and Sharing
 _  MOUNT            0       0  Effective UNIX mount points
 _  SENSAPF          1     337  APF data set names
 _  SENSLINK         1      65  Linklist data set names
 _  SENSLPA          1      24  LPA list data set names
 _  SENSALL          1     980  All sensitive data sets by priority and type
 _  SETROPTS         1       1  RACF system, ICHSECOP, and general SETROPTS settings
 _  SETROPAU         2      22  SETROPTS settings - audit concerns
 _  ROUTER           1       2  SAF router table (ICHRFR01)
 Command ===> _____  Scroll===> CSR
 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
MA      a                                                          04/001
```

Automated Vulnerability Assessment

SMF "exceptions" report


```
Session A - [32 x 80]
zSecure Audit for RACF Display Selection          29 s elapsed, 20.3 s CPU

    Name       Summary Records Title
_   USEOPER        3      376 Use of OPERATIONS Attribute
_   CMDSPEC        4      155 Commands issued by SPECIAL users
_   CMDFAIL        3        9 Command violations
_   AUDUSER        2     5815 Auditing of Users
_   DSETVIOL      11       24 Data Set Access Violations by Profile and User
_   GRESVIOL       3       17 General Resource Access Violations by Class, Profile
_   VWBYUSER       9       41 Violations and Warnings by User
_   LOGTERM        0        8 Attempted Logon by Pwd/Userid Guessing, > 5 per Term
_   LOGUSER        0        8 Attempted Logon by Password Guessing, > 5 per Userid
_   LOGREVK        1        2 Attempted Logon by Revoked User
_   LOGATTN        0        1 Attempted Logon, attention required
****************************** Bottom of Data ******************************









Command ===> _                                              Scroll===> CSR
MA    a                                                              32/015
```
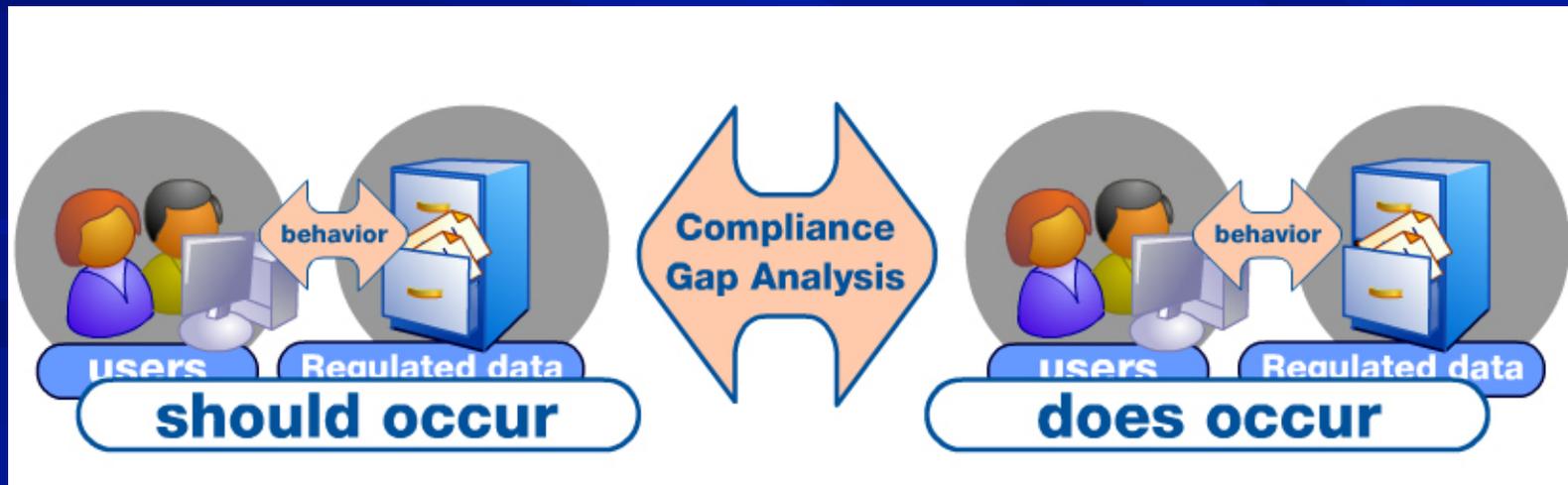
Status Auditing

What Can Happen!

- Shows definitions, like all users with system special

- Large amount of output, hopefully every day the same

What we want to happen!

- Exceptions summarised in an email
- Detail reports available for review and archiving
- Needs to be resource efficient & scalable

What we want to happen!

- **Change detection**
  - Detect differences with previous reporting run
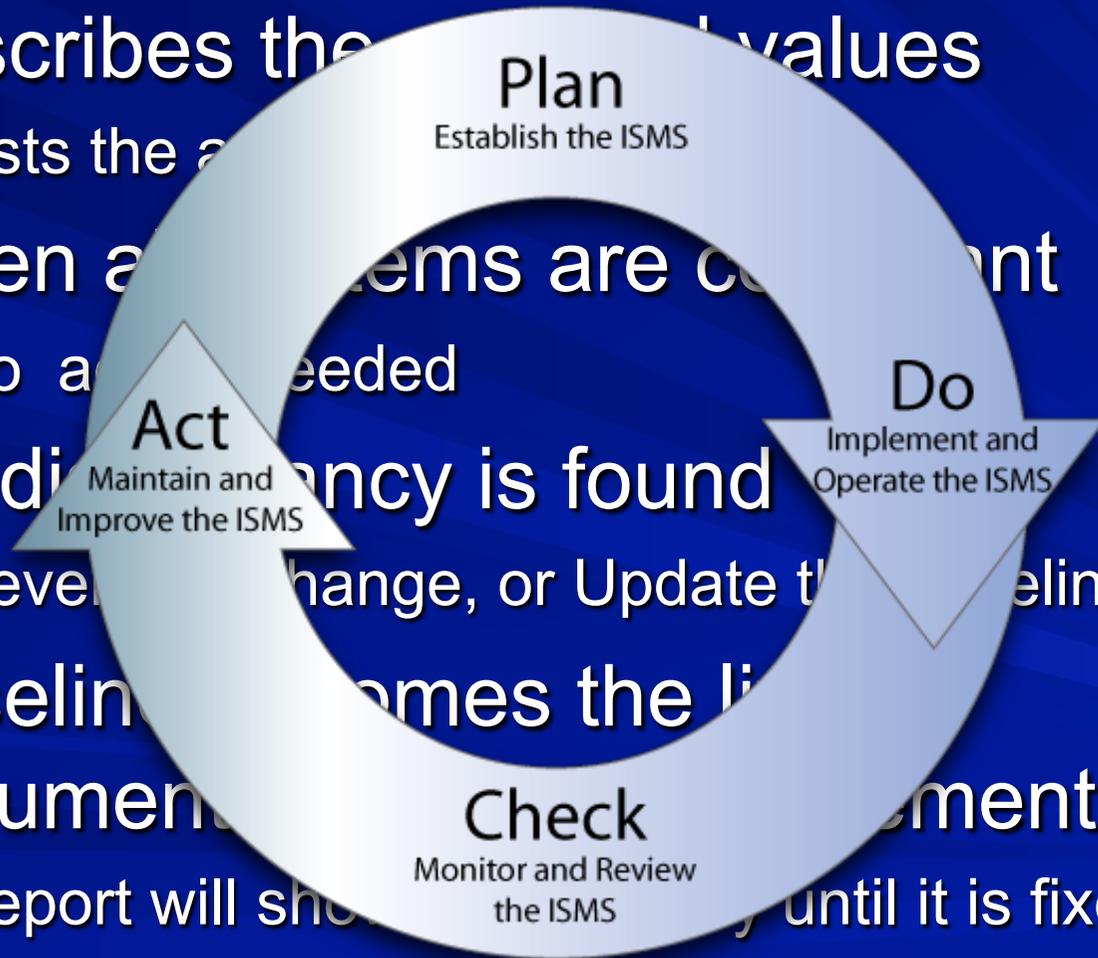 - Changes may be missed when a report was skipped/lost
- **Baseline verification**
  - Shows when the definitions do not fit the standards
  - Typically by comparing the status against a baseline
- **Automation allows you to move from "Auditing" to "Monitoring"**

- **Describes the** **values**
  - Lists the **a** **...**
- **When a** **ems are c** **nt**
  - No **ac** **eded**
- **If a di** **ncy is found**
  - Rever **ange, or Update t** **eline**
- **Baselin** **mes the li**
  document **mentation**
  - Report will sho **until it is fixed**

Plan
Establish the ISMS

Do
Implement and Operate the ISMS

Act
Maintain and Improve the ISMS

Check
Monitor and Review the ISMS

How Can we automate?

- Compliance requirements
  - Monitor changes to operating system and security
  - Monitor activities of privileged users
  - Monitor irregular logons
  - Verify operating system parameters against baselines
  - Verify users with specific (high) application authority

How can we automate?

- **zSecure Audit customised reporting:**
  - Built with CARLa report specification
  - Using your policy and naming conventions
  - Baselines document the security implementation standards
  - Show parameters that are in conflict
  - Approved changes must be reflected in the baseline
  - Inappropriate changes will show up until they have been addressed

View for the Compliance Manager

Security Monitor summary for RACF reports generated on: 11 Jun 2007 - Lotus Notes

Please respond to Security Management Team

To: Compliance and Security Management Team
cc: Change Management Team
bcc:
Subject: Security Monitor summary for RACF reports generated on: 11 Jun 2007

Default custom expiration date of 10-06-2008

```
Security Monitor summary for RACF reports generated on: 11 Jun 2007

     13 Accounts that were last used 60...90 days ago on system: DEMO
   2656 Accounts that were last used >90 days ago on system: DEMO
     19 Userids with an non-expiring password on system: DEMO
    236 New or incompliant started tasks on system: DEMO
     59 Unknown/Unverified accounts with system level attributes on system
     29 Unknown/Unverified accounts with UID=0 on system: DEMO
     13 Profiles in WARNING mode for system: DEMO
     12 Unknown/unverified global access checking table entry on system: D
     65 Unknown/Unverified group level privileged accounts on system: DEMO
        All systems have compliant RACF dataset profiles
    322 New/unverified/incompliant dataset profiles found on system: DEMO
        RACF Authorized Caller Tables are empty, compliant to Baseline
      7 Unknown/Unverified active EXIT(s) found on system: DEMO
      2 RACF database name, location or attributes changed on system: DEMO
        All SPT entries are compliant to the Baseline
    198 Non-compliant resource class setting on system: DEMO
    125 Non-compliant PPT entries on system: DEMO
     16 Non compliant RACF SETROPTS settings system: DEMO
      1 Non-compliant z/OS General Setting on system: DEMO
```

Subject of message.

Could not find 'Change Management Team'   Disconnected   IBM ID

View for the Technician


```
Session B - [32 x 80]                                                    _ □ ✕

   Menu   Utilities   Compilers   Help

 BROWSE      DEMO.COMPLIAN.REPORTS                    Line 00000000 Col 001 080
********************************* Top of Data **********************************
Non compliant RACF SETROPTS settings system: DEMO

SETROPTS setting description    Current            Desired
Batch userid req BATCHALLRACF   Yes                No
Default uid local  UNDEFINEDU   ++++++++           ?UNKNOWN
Default uid remote  NJEUSERID   ????????           ?NJEDUMM
Enhanced Generic Naming         No                 Yes
Key change required day         None                30
Password change interval         90                 30
Password change warning day     No                  7
Password rule 1                 ******** LENGTH(5:8) LLLLLLLL LENGTH(8:8)
Prefix one-level dsns           ONEQUAL            SINGDSN
Prevent logon if unused days    255                180
Prevent uncataloged dsns        Yes/fail           No
Real datasetnames in SMF        Yes                No
Revoke after password attempt    5                  3
Tape dataset check TAPEDSN      Yes                No
Tape volume protection active   Yes                No
Undefined terminal TERMUACC     NONE               READ
******************************** Bottom of Data ********************************




 Command ===>                                             Scroll ===> CSR
MA    b                                                                 32/015
```

Cost Effective Automated Mainframe Security

Automatic Enforcement

What Do We Do Today?

- **Situation:**
  - Security management outsourced
  - User administration delegated to non-technical users
  - Departments with their own applications, responsibility and security administrators

  - Way too many Group & System Special Users!!

What Do We Do Today?

- **Solutions Available:**
  - Implement GROUP SPECIAL or GROUP AUDITOR
    - Impractical when profile ownership is not clearly specified in RACF
  - ISPF front end to build RACF commands
    - Users do not key in RACF commands, but privilege is not protected

zSecure Option

- RACF command screening using zSecure Command Verifier
  - Each security change verified against granular policy
    - Using masks for classes and profiles
  - Inappropriate commands prevented
  - Missing or incorrect parameters can be fixed
  - Even controls commands issued by system special users

Command Verifier – Example 1

- All controlled via profiles defined in the RACF XFACILIT class
- If you forget to code an OWNER, take first 3 letters of userid as OWNER

```
Profile                 APPLDATA         UACC

C4R.USER./OWNER.**      =USERID(3)       READ
```

Command Verifier – Example 2

- Do not allow the use of the TRUSTED and PRIVILEGED keywords

```
Profile                                          UACC


C4R.STARTED.STDATA.ATTR.PRIVILEGED.**      NONE
C4R.STARTED.STDATA.ATTR.TRUSTED.**         NONE
```

The Results .. ta da……


```
Session A - [24 x 80]

setr password(nohistory)
 C4R751E SETROPTS PASSWORD.HISTORY not allowed, command terminated
 READY
setr password(interval(180))
 C4R751E SETROPTS PASSWORD.INTERVAL not allowed, command terminated
 READY
permit irr.password.reset class(facility) id(ibmuser) access(update)
 C4R607E ACL setting for self to UPDATE not allowed, command terminated
 READY
ralter facility irr.password.reset uacc(update)
 C4R600E UACC UPDATE setting not allowed, command terminated
 READY
setropts noclassact(facility)
 C4R754E CLASSACT not allowed for class FACILITY, command terminated
 READY
permit 'sys1.parmlib' gen id(ibmuser) access(update)
 C4R646E Management of locked profiles not allowed, command terminated
 READY
connect ibmuser group(sys1)
 C4R548E You may not connect yourself to group SYS1, command terminated
 READY
_

MA    a                                                              22/001
```

Command Audit Trail

Command Audit Trail - What

- Keep track of significant changes to profiles
  - Adding/changing/deleting application segments
    - like OMVS, TSO, CICS and STDATA
  - Adding/removing user attributes
    - like Special, Operations, Restricted
  - Connecting/removing users from groups
  - Adding/removing attributes for datasets and general resources
  - Permit commands for datasets and resources adding/deleting members on resource profiles
    - the last 64 additions/changes/removals will be tracked

Command Audit Trail - Why

- Answer questions like
  - Since when does this user have TSO authority?
  - Who gave this user Special?
  - Since when has this Group/User access to this dataset?
  - Was anything changed in the access list of this resource recently?
  - Who put this profile in warning mode, and when did (s)he do it?

Command Audit Trail - When

- Maintained when activation profile exists
  - C4R.class.=CMDAUD.data-type.more
  - Data-type is
    - =SEGMENT - adding, changing and deleting segments
    - =ATTR - adding and deleting attributes
    - =CONNECT - adding, changing and deleting user to group connections
    - =ACL - use of the PERMIT command
    - =MEMBER - adding and deleting members in a grouping resource class profile
  - E.g. C4R.DATASET.=CMDAUD.=ACL.**
    - Permits, UACC etc. on activation profile are ignored

Command Audit Trail - Where

- **Kept within the target profile, in USRDATA**
  - Not replicated with RRSF
- **Display using:**
  - LISTUSER, LISTGRP, LISTDSD, RLIST
  - C4RCATMN command

```
____ C4RCATMN _____
|                                                                            |
|          _LIST___                                                          |
|        _|_____|__CLASS(class)__PROFILE(profile)__ _____ _           |
|        | |_REMOVE_|                                 |_GENERIC_| |          |
| >>__|__|_____|_____><  |
|        |_MSG_____|            |
|        |_NOMSG_____|            |
|                                                                            |
|_____|
```

Command Audit Trail – List

- List the whole audit trail
  - UPDATE on the activation profile

```
c4rcatmn list class(user) profile(ibmuser)

Command Audit Trail for USER IBMUSER
Segment:  CICS     Added on 05.241/03:19 by C4RTEST
                   Changed on 05.241/03:20 by C4RTEST
          TSO      Changed on 05.241/03:19 by C4RTEST
Attrib:   PASSWRD Removed on 05.238/14:24 by C4RTEST
          INTERV  Changed on 05.241/04:42 by C4RTEST
          RESTR    Added on 05.238/14:24 by C4RTEST
Connect:           BCSC Added on 05.238/14:24 by IBMUSER
GrpAttr:  ADSP     BCSC Removed on 05.238/14:24 by IBMUSER
```

```
| Command Audit Trail for USER IBMUSER
| Segment:  CICS     Added on 05.241/03:19 by C4RTEST
|                    Changed on 05.241/03:20 by C4RTEST
|           TSO      Changed on 05.241/03:19 by C4RTEST
| Attrib:   PASSWRD  Removed on 05.238/14:24 by C4RTEST
|           INTERV   Changed on 05.241/04:42 by C4RTEST
|           RESTR    Added on 05.238/14:24 by C4RTEST
| Connect:           C4RGRP1 Added on 05.238/14:24 by IBMUSER
| GrpAttr:   ADSP    C4RGRP1 Removed on 05.238/14:24 by IBMUSER
|
|
| Command Audit Trail for DATASET  IBMUSER.**
| Segment:  DFP     Added on 05.245/05:21 by C4RTEST
| Attrib:   WARNING Added on 05.245/05:20 by C4RTEST
| Access:           C4RGRP1 access READ on 05.234/09:39 by C4RTEST
|                   C4RGRP2 access READ on 05.234/09:39 by C4RTEST
|                   C4RTEST access READ on 05.234/09:39 by C4RTEST
|                   SYS1 access READ on 05.234/09:39 by C4RTEST
|                   IBMUSER access READ on 05.234/09:39 by C4RTEST
|                   * access UPD on 05.234/09:39 by C4RTEST
|                   CRMBGUS access Removed on 05.234/09:39 by C4RTEST
|                   **ALL** access Removed on 05.257/15:06 by IBMUSER
|
|
| Command Audit Trail for GCICSTRN CICSA.SPRO
| Member:           CICSA.CEDA Added on 05.249/14:21 by C4RTEST
|                   CICSA.CEMT Removed on 05.249/14:21 by C4RTEST
|
|
```

Cost Effective Automated Mainframe Security

Automating Manual Processes

Generating RACF Commands

- Perhaps the most straight forward function provided by zSecure Admin
- Ability to generate large amounts of RACF commands in a timely manner
- Simple task of cloning a RACF group can require 100's of commands
  - ADDGROUP
  - CONNECT's
  - PERMITS

Generating RACF Commands

- Can be done via:
  - ISPF interface
  - CARLa Code Interactively
  - CARLa Code in batch

Group Selection Panel in ISPF

```
                              zSecure Admin+Audit for RACF - RACF - Group Selection
Command ===> _____ _ start panel


_    Add new group or segment


Show groups that fit all of the following criteria
Group id  . . . . . PMI_____       (group profile key or filter)
Owner . . . . . . . _____         (group or userid, or filter)
Subgroup of . . . . _____         (group or filter)
With subgroup . . . _____         (group or filter)
Installation data . _____ (data scan, no filter except *)


Additional selection criteria
_   Profile fields      _   Connect fields    _   Segment presence  _   Absence


Output/run options
_   Show segments       _   All              _   Expand universal  _   Specify scope
_   Print format            Customize title      Send as e-mail
        Background run       Full detail form     Sort differently     Narrow print
        Print connects       Print names          Print subgroups
```

Copy Group

```
zSecure Admin+Audit for RACF GROUP PMI Overview          0 s elapsed, 0.0 s CPU
Command ===> _____ Scroll===> PAGE
like PMI                                            21 Feb 2008 17:35
   Group      Complex   SupGroup X Owner      Grps    Users   Conn U nTU Created
C  PMI        ED02      CRMTRAIN   CRMTRAIN      4        4       4    ___ 08Jun2007
*************************** Bottom of Data ***************************************
```

```
                zSecure Admin+Audit for RACF - RACF - Group Copy
Command ===> _____


From group  . . . . PMI
To id . . . . . . . PMID


OMVS gid  . . . . . _____      (numeric id(suffix S for SHARED) or AUTO)


_    Generate RACF commands even when the target group exists
_    Copy permits only (target id may be a group or a user)


Specify options for new group
_    Copy catalog aliases (only if CKFREEZE is present)
_    Issue ADDSD/RDEF for user resources
  _    Copy RACFVARS profiles/members too (if option above selected)
```

Copy Group Return Code

```
zSecure Admin+Audit for RACF  GROUP PMI Overview         Commands queued, RC=4
Command ===> _____    Scroll===> PAGE
like PMI                                         21 Feb 2008 17:48
   Group      Complex  SupGroup X Owner        Grps    Users   Conn U nTU Created
__ PMI        ED02     CRMTRAIN   CRMTRAIN        3        4      4   ___ 08Jun2007
******************************* Bottom of Data ********************************
```

Generated Commands

```
EDIT        ORI.C2R1FD8.CKRCMD                      Columns 00001 00072
Command ===> _____    Scroll ===> PAGE
****** ***************************** Top of Data *****************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001          /* CKRCMD file CKR1CMD complex ED02 NJE TVT4107 generated 21 Fe
000002          /* CKRCMD file CKR1CMD complex ED02 NJE TVT4107 generated 21 Fe
000003          /* Commands generated by COPY USER/GROUP    */
000004        addgroup PMID      +
000005          data('Drama admin group') +
000006          owner(PMI) supgroup(PMI)
dd0007        connect TOMZEEH  group(PMID) owner(PMID)   auth(USE) uacc(NONE)
000008          /* Commands generated by COPY PERMIT        */
000009        permit STGADMIN.IGG.DEFDEL.UALIAS cl(FACILITY) ac(READ) id(PMID
000010        permit MVS.START.STC.PMIX.** cl(OPERCMDS) ac(UPDATE) id(PMID
000011        permit ISFOPER.SYSTEM cl(SDSF    ) ac(READ) id(PMID     )
000012        permit PMIOPER.SUBMIT cl(SURROGAT) ac(READ) id(PMID     )
000013        permit 'CRMBERT.TRT.**' generic ac(NONE) id(PMID     )
000014        permit 'PMI.**' generic ac(READ) id(PMID     )
dd0015        permit 'PMI.CKFREEZE' generic ac(ALTER) id(PMID     )
```

Running the Generated Commands

```
                      zSecure Admin+Audit for RACF   Enter R to run commands
Command ===> _____


The following selections are supported:
 B Browse file                      S Default action (for each file)
 E Edit file                        R Run commands
 P Print file                       J Submit Job to execute commands
 V View file                        W Write file into seq. or partitioned data set
 M E-mail report


Enter a selection in front of a highlighted line below:
_   SYSPRINT   messages
_   REPORT     printable reports
_   CKRTSPRT   output from the last TSO command(s)
R _ CKRCMD     queued TSO commands
_   CKR2PASS   queued commands for zSecure Admin+Audit for RACF
_   COMMANDS   zSecure Admin+Audit for RACF input commands from last query
_   SPFLIST    printable output from PRT primary command
_   OPTIONS    set print options
```

Command Output

```
BROWSE       SYS08088.T133434.RA000.INST001.R0100427      Line 00000001 Col 001 080
Command ===>                                                   Scroll ===> 1

================================================================
=== Multiple TSO command output file - scroll max down for overview ===
=== Input data set INST001.C2R1E05.CKRCMD                     ===
================================================================
/* CKRCMD file CKR1CMD complex RCOD generated 28 Mar 2008 13:34 */
/* CKRCMD file CKR1CMD complex RCOD generated 28 Mar 2008 13:35 */
/* No CKFREEZE present, no resource copying commands will be generated */
/* Commands generated by COPY USER/GROUP    */


============ 28Mar08 13:37:53.67719 start record 5 ============
addgroup PMID     data('Drama admin group') owner(PMI) supgroup(PMI)


============ 28Mar08 13:37:53.76738 start record 8 ============
addgroup PMIDU    data('Drama user group') owner(PMID) supgroup(PMID)


============ 28Mar08 13:37:53.83565 start record 11 ============
addgroup PMIDR    data('Drama resource group') owner(PMID) supgroup(PMID)
================================================================
=== All commands completed successfully                      ===
================================================================
```

Cost Effective Automated Mainframe Security

Other Functions

Other Functions

- Given we only have an one hour not enough time to cover all facilities available:
  - zSecure Alert
  - Access Monitor
  - RACF Offline
- So one slide on each……

zSecure Alert

- **Situation**
  - Too many technicians with access to business databases
  - Must keep financial data confidential to prevent insider trading
  - Allow technicians to do their work

- **Real-time alert as mitigating control using zSecure Alert**
  - Reduce need to implement separation of access
  - sysprogs keep their "must be able to read/change anything" status
  - No need for political battle or costly re-orgs
 - Quick install, instant visibility

Access Monitor

- Situation
  - Profiles from old applications
  - Permits and connects from previous job
  - CICS transactions, no longer needed
  - Must fix profiles to fit current needs
  - PCI-DSS, SOX, HIPAA, etc all demand appropriate authorities
- zSecure Admin, Access Monitor
  - Logs RACF access decisions efficiently
  - Identifies unused profiles, groups, permits, members
  - Generates RACF commands to delete

RACF Offline
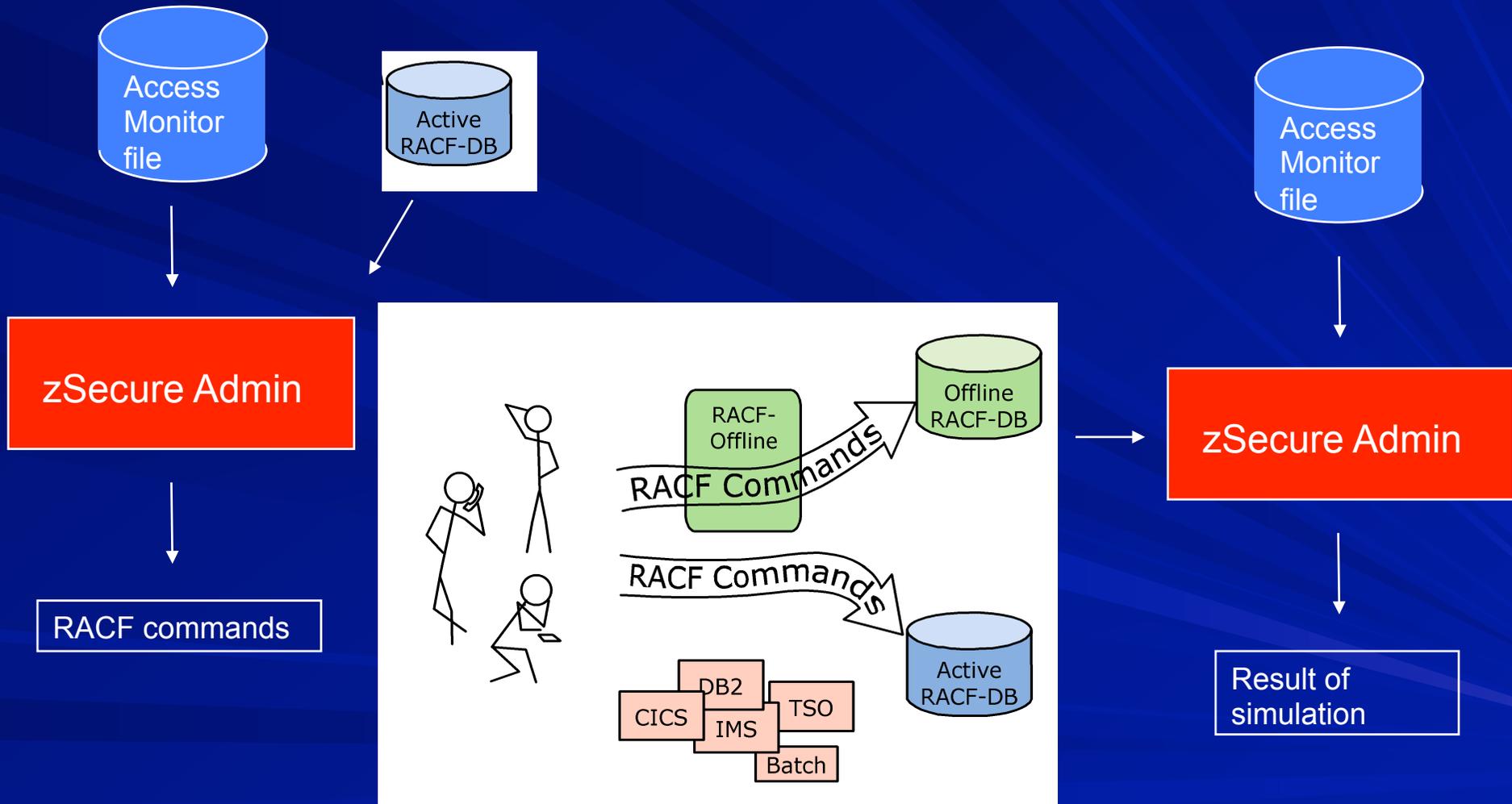
Cost Effective Automated Mainframe Security

Summary

Summary

- Using the out of the box facilities provided by the zSecure product suite it is possible to vastly improve the security posture of your system z estate

- With a little time and effort you can implement effective security controls that will assist in meeting all of your compliance & audit requirements

- You will also make your technical, administration and audit teams extremely effective when it comes to system z security management

Questions?

Reference Material

- zSecure Homepage:
  http://www-01.ibm.com/software/tivoli/products/zsecure/
- zSecure information center:
  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc/welcome.html
- zSecure release note information:
  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc/releaseinfo/releaseinformation.html
- zSecure forum:
  http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1255
- zSecure Redbook:
  http://www.redbooks.ibm.com/abstracts/sg247633.html?Open
- zSecure Quarterly Newsletter:
  (send e-mail to jamie_pease@uk.ibm.com to join)

Contact Details

Mark Wilson
RSM Partners

Markw@rsmpartners.com

Mobile +44 (0) 7768 617006

www.rsmpartners.com