Quick Start Your zSecure Suite - LAB

Mark S Hahn
IBM

Monday, August 6, 2012
Session 11687

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

ibm.com/security

From the Top

- Install the product(s)
  - Determine which products are to be used
- Ensure product is not DISabled
  - Review IFAPRDxx
- Control access to key resources
  - Function
  - Menu Building
  - Options available

Signing on

- PCOMM – Personal Communicator
- Application TSO
- Log onto the system
  - SHARA20
  - SHARA21
  - SHARA22
  - SHARA23
  - SHARA24
  - SHARA25
- Password is: (instructor provided)

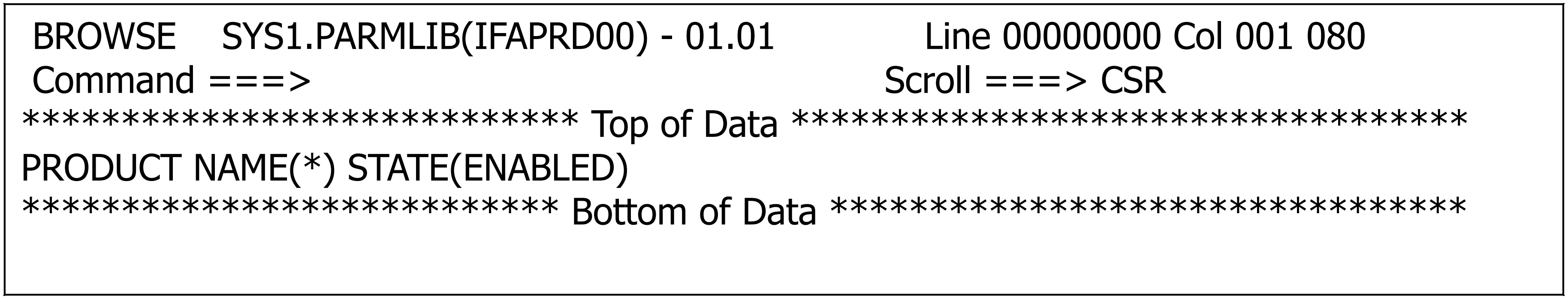
Signing On

- ISPF option 6 – TSO commands
- CKR

IFAPRDxx – Product Enablement

- zSecure defaults to enabled
- IFAPRDxx used for DISabling

- Go review SYS1.PARMLIB(IFAPRDxx)



```
 BROWSE    SYS1.PARMLIB(IFAPRD00) - 01.01             Line 00000000 Col 001 080
 Command ===>                                              Scroll ===> CSR
**************************** Top of Data **********************************
PRODUCT NAME(*) STATE(ENABLED)
*************************** Bottom of Data ********************************
```

Bare Minimum Profiles

- Create catchall profiles with UACC=NONE
  - CKF.**
  - CKG.**
  - CKR.**
  - C2R.**
  - **NOT C4R.****
  - TOOLKIT.**

- grant READ access to the people entitled to use all functions of zSecure
- **NOTE**: a wider generic profile like *.** is not sufficient
- **NOTE:** zSecure requires the IRR.** FACILITY class profile

Setting up for CKFREEZE

- CKFREEZE (program: CFKCOLL) gathers data to be analyzed later – snapshots the system
- zSecure RA.R for class XFACILIT

```
CKF.ADMIN                                    NONE
CKF.ALERT                                    NONE
CKF.AUDIT                                    NONE
CKF.TCIM                                     NONE
CKF.VISUAL                                   NONE
```

- Determines if user allowed to perform function.
- Broken out by product
- Appendix B in <u>Installation and Configuration Guide</u>

Setting up for CKFREEZE

- First we'll do a setup files
  - SE.1
  - _I_Active backup RACF data base and live SMF data sets

```
 zSecure Admin+Audit for RACF - Setup -
Command ===>


Description . . . . Your description for this input file

. . . .
 Data set name or DSNPREF=, or Unix file name    Type
_______________________________________________  CKFREEZE
*********************** Bottom of data *******************
```

Define and create CKFREEZE

- Name the (non-)existent data set and set to CKFREEZE

```
  Data set name or DSNPREF=, or Unix file name              Type
 data.ckfreeze                                            ckfreeze
********************** Bottom of data ***********************
```

- Enter

```
CKFREEZE file not found. Change dataset name, or specify allocation parameters

 Dataset name . . . 'SHARA25.CKFREEZE.DATA'

Allocation parameters to create new dataset:
 Volume serial  . .             (Blank for authorized default volume)
 Generic unit . . .             (Generic group name)
 Space units  . . .  CYLS       (KB, MB, TRKS, or CYLS)
 Primary quantity .     1       (In above units, press HELP . .
 Secondary quantity     1       (In above units)
```

Populate CKFREEZE

- F3
- F3
- Put an F next to your fileset (description)

```
Fill in jobcard information:
Option ===>

1   View           View JCL
2   Edit           Edit JCL
3   Submit         Submit JCL for execution
4   Cancel         Do not submit the JCL
5   Parameters     Specify zSecure Collect parameters

Job statement information:  (Verify before proceeding)
> //SHARA25C JOB CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
>
```

CKF.** for CKFCOLL

- Run a REFRESH for CKFREEZE

```
********************************* TOP OF DATA ******************************
                         J E S 2  J O B  L O G  --  S Y S T E M  S 1      --

16.45.26 JOB02105 ---- THURSDAY,  02 AUG 2012 ----
16.45.26 JOB02105  IRR010I  USERID SHARA25  IS ASSIGNED TO THIS JOB.
16.45.26 JOB02105  ICH70001I SHARA25  LAST ACCESS AT 16:37:27 ON THURSDAY, A
16.45.26 JOB02105  $HASP373 SHARA25A STARTED - INIT 6    - CLASS A - SYS S1
16.45.27 JOB02105  ICH408I USER(SHARA25 ) GROUP(SHARUSER) NAME(SHARE USER
   991               CKF.AUDIT CL(XFACILIT)
   991               INSUFFICIENT ACCESS AUTHORITY
   991               ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )
16.45.27 JOB02105  ICH408I USER(SHARA25 ) GROUP(SHARUSER) NAME(SHARE USER
   992               CKF.ADMIN CL(XFACILIT)
   992               INSUFFICIENT ACCESS AUTHORITY
   992               ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )
```

Clean up

- Go to 3.4
- Type in your userid
- Find your CKFREEZE.DATA dataset
- / in action column
- Choose Delete

- Setup Files
- ‘E’dit your fileset
- Replace dsname with 'SHARE.ZSEC12.LAB.CKFREEZE‘
  - DON’T FORGET THE quotes (‘)

CKF.* profiles

- Needed for whichever products you want to collect data for
- zSecure Alert
  - Collection job userid
    - CKF.ALERT
    - CKF.COLLECT

CKR.** profiles

- Determines which displays can be seen by user
- Who is allowed to see all RACF database records?
  Give only central administrators READ permits.

```
CKR.READALL                NONE
```

- Who is allowed to invoke CKRCARLA in APF-authorized mode?

```
CKR.CKRCARLA.APF           NONE
```

Menu controls

- Frequent ‘gotcha’
- Symptom: blank or omitted lines from Menu
- The resource names follow the same naming convention:
  - first qualifier: 'CKR'
  - second qualifier: 'OPTION' / ‘ACTION’
  - third qualifier: main panel option
  - fourth qualifier: secondary menu option etc.

  - So for the main panel, the resource names are:
    - CKR.OPTION.SE.1 for SETUP FILES
    - CKR.OPTION.RA for RACF

- CKR.OPTION.** UACC(NONE)
- CKR.ACTION.** UACC(NONE)

- Exercise –
  - What menu options are controlled?
  - Useful for Helpdesk menu tailoring

CKGRACF controls

The CKGRACF user does not require any special RACF authority such as the SPECIAL or group-SPECIAL attribute. The CKGRACF program, using APF interfaces, adopts whatever authority it needs for a task. Therefore, you must control who can use the CKGRACF program by putting each CKGRACF user or group of users in the access control lists of several XFACILIT class profiles.

- Ensure CKG.** with UACC(NONE) is defined
- Very extensive guide for CKG profiles in Audit/Admin User Guide: Chapter 14

zSecure Toolkit for CICS

- 1. Define the Toolkit SVC to RACF with the RDEFINE command.

```
RDEFINE FACILITY TOOLKIT.SVC UACC(NONE)
```

- 2. Grant SVC access to each CICS region that will have an installation of the toolkit.

```
PERMIT TOOLKIT.SVC CLASS(FACILITY) ID(userid)
  ACCESS(READ)
```

  - where *userid* is the ID of the CICS region.
- 3. Build the generic block:

```
RDEFINE FACILITY TOOLKIT.** UACC(NONE)
```

- 4. Define the specific functions to users

zSecure CICS Toolkit

- Review your site
  - CKR
  - RA.R (RACF Resources)
    - Class: FACILITY (not XFACILIT)
    - Profile: TOOLKIT.**
  - Check for TOOLKIT.SVC
    - UACC(NONE)
    - Permit CICS regions
  - Check for TOOLKIT.** (or 4 letter transaction codes)

zSecure Command Verifier

- Control who has access
  - **C4R.EXEMPT** – UPDATE or higher is uncontrolled!!

- This profile specifies to display the command that is passed to RACF before executing it. Use only the READ access level at this time.
  - **C4R.DEBUG NOTE:** This profile is now deprecated. Instead, use the C4R.=MSG.CMD profile.
  - **C4R.=MSG.CMD**

zSecure Command Verifier

- Review your site
  - CKR
  - RA.R (RACF Resources)
    - Class: XFACILIT
    - Profile: C4R.**
  - Watch for any WARNING (Y) profiles
    - zSecure Command Verifier does not support the use of warning mode on policy profiles
  - Check for C4R.** profile – NOT recommended
  - Check for C4R.EXEMPT
    - Is anyone above the rules?

Summary

- Starting up with zSecure
  - IFAPRDxx not required to enable
  - Appendix B in Installation and Configuration Guide
  - CKF.** - CKFCOLLECT - CKFREEZE
  - CKG.** - CKGRACF – special command handler
  - C2R.** - authorization with Audit / Admin
  - NOT C4R.** - Command control over all
  - TOOLKIT.** - CICS interface to zSecure

Thank you

- Please submit your session evaluations

11687

  - Online at SHARE.org/AnaheimEval
  - Paper copy if needed