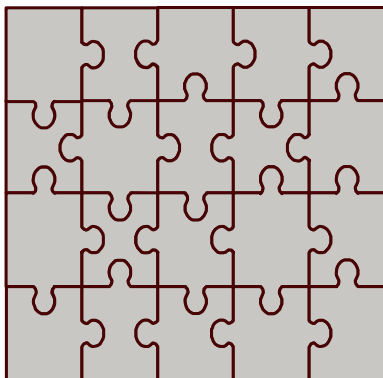


RACF Level 2 UPDATE

-- a Diagnostic Approach



New York RACF User's Group
Thursday October 29th, 2003
New York City



Russ Hardgrove
RACF Level 2 Team Leader
IBM - OS/390 & z/OS Software Service
Poughkeepsie, NY 12601
hardgrov@us.ibm.com



Agenda

- SAFTRACE Facility
(z/OS VIR2 -very brief overview)
- Locating the caller of RACF
- ICH408I - get the WHOLE message
- The caller versus RACF
- Current APARS of some interest
- Miscellaneous info
- Level2 Personnel
- Some questions and [hopefully] answers



SAFTRACE Facility

- z/OS VIR2
- Traces:
 - RACROUTEs (Auths, Verifies, etc.)
 - Manager calls (ICHEINTYs)
 - OMVS Callable Services
 - Doesn't trace branch entered services
- Use SET command to initiate, filter stop
- GTF required to be running
- RACF Address space required
- Requirements (a good knowledge of)
 - RACF parameter lists
 - RACF in general
- Two trace records - pre / post event
- Practice makes perfect - (become familiar before first fire - needed use)

Locating the caller of RACF service

- Easiest when an SVC was issued by caller
 - hardly used anymore.
 - pickup PSW from SYSTRACE or the RB in SUMM FORMAT.
 - RI has Parameter list of call.
- Most common call is RACROUTE
 - uses BALR 14,15
 - need to use R0 (points to 2 words).
 - Need to go back thru SAF PL/saveareas.
 - get R0 from either SYSTRACE entry or the next RB in SUMM FORMAT.
- We won't be covering OMVS callable services calls in this presentation.

Locating the caller of RACF service

- example from a RACROUTE

```

)5 00A2 009DD928   SVC      82   070C2000 80DA266E  00000000 00005910 00000000
)5 00A2 009DD928   SVC      77   070C2000 88203442  88201FE4 FFF00000 000E0001
)5 00A2 009DD928   SVCR    77   070C2000 88203442  00000000 FFF00000 80004000
  
```

IPCS OUTPUT STREAM -----

Command ==> **ip where 00DA266E**

```

*****
ASID(X'00A2') 00DA266E. ICHRF00+266E IN PLPA
*****
  
```

SVRB: 009FF928

```

-0020 XSB..... 7FFFC918  FLAGS2... 00          RTPSW1...
-0008 FLAGS1... 02000000  WLIC..... 00020082
+0000 RSV..... 00000000  00000000          SZSTAB...
+0018 Q..... 00000000  LINK..... 009DD8A0
+0020 GPR0-3... 00000000  009B8A5C  009ACED9  009CA480
+0030 GPR4-7... 009CAE30  009AA688  009C9340  009D6F08
+0040 GPR8-11.. 009B88B8  07F3C2F5  07F3B2F6  07F3A2F7
+0050 GPR12-15. 87F392F8  009B88B8  87F3B2C6  00000000
  
```

SVRB: 009FF738

```

-0020 XSB..... 7FFFC7B8  FLAGS2... 80          RTPSW1...
-0008 FLAGS1... 02000004  WLIC..... 00040010
+0000 RSV..... 00000000  00000000          SZSTAB...
+0018 Q..... 00000000  LINK..... 009FF928
+0020 GPR0-3... 00005910 00000000  00DA1C50  00F4B530
+0030 GPR4-7... 00000002  00000001  00000001  00005A90
+0040 GPR8-11.. 00005A28  00005888  00000000  00005890
+0050 GPR12-15. 00DA1C50  00005890  00000002  00000000
  
```

ASID(X'00A2') STORAGE -----

Command ==> **1 00005910**

```

)0005910  00005A90 00005A28 00000000  884C68B2  | ..!...!.....h<.. |
)0005920 TO 000059FF (X'000000E0' bytes)--All bytes contain X'00'
)0005A00  00000000  00005A90  00000000  00000000  | .....!..... |
)0005A10 TO 00005A2F (X'00000020' bytes)--All bytes contain X'00'
)0005A30  00AC0000  00010000  00000000  00000000  | ..... |
  
```

Locating the caller of RACROUTE

```
ASID(X'00A2') STORAGE -----  
Command ==> First word is address of RACF parameter list  
00005910 ? 00005A90 00005A28 00000000 884C68B2 | ..!...!.....h<.. |  
00005920 TO 000059FF (X'000000E0' bytes)--All bytes contain X'00'  
00005A00 00000000 00005A90 00000000 00000000 | .....!..... |  
00005A10 TO 00005A2F (X'00000020' bytes)--All bytes contain X'00'  
00005A30 00AC0000 00010000 00000000 00000000 | ..... |
```

```
ASID(X'00A2') STORAGE -----  
Command ==>  
00005A90 44000000 98000000 04000000 00000000 | ....q..... |  
00005AA0 TO 00005AAF (X'00000010' bytes)--All bytes contain X'00'  
00005AB0 00000000 00005AF8 00005B24 00005B2C | .....!8..$...$. |  
00005AC0 TO 00005AEF (X'00000030' bytes)--All bytes contain X'00'
```

```
ASID(X'00A2') STORAGE -----  
Command ==> Second word is address of SAF parameter list  
00005910 00005A90 ? 00005A28 00000000 884C68B2 | ..!...!.....h<.. |  
00005920 TO 000059FF (X'000000E0' bytes)--All bytes contain X'00'  
00005A00 00000000 00005A90 00000000 00000000 | .....!..... |  
00005A10 TO 00005A2F (X'00000020' bytes)--All bytes contain X'00'  
00005A30 00AC0000 00010000 00000000 00000000 | ..... |
```

```
ASID(X'00A2') STORAGE -----  
Command ==> from here issue l x+18?+14?+c (explained in 3 pages)  
00005A28 TO 00005A2F (X'00000008' bytes)--All bytes contain X'00'  
00005A30 00AC0000 00010000 00000000 00000000 | ..... |  
00005A40 00005828 00000000 00000000 00000068 | ..... |  
00005A50 TO 00005A8F (X'00000040' bytes)--All bytes contain X'00'  
00005A90 44000000 98000000 04000000 00000000 | ....q..... |  
00005AA0 TO 00005AAF (X'00000010' bytes)--All bytes contain X'00'
```

Locating the caller of RACROUTE

ASID(X'00A2') STORAGE

Command ==>

00005398			884C68B2	00D9A000	.	h<...R..	
000053A0	08150008	10745064	00280000	08150008	&.....	
000053B0	00000001	10745000	00005818	00005828	&.....	
000053C0	10745000	00FBE700	084C770B	000052F0		..&...X..<.....0	
000053D0	884C670C	00000000	00000000	00000000		h<.....	
000053E0	TO 000053FF (X'00000020' bytes)--All bytes contain X'00'						

CALLED (where you're headed)

IPCS OUTPUT STREAM -----

Command ==> **ip where 00D9A000 reg 15 (to addr)**

ASID(X'00A2') 00D9A000. ICHSFR00+00 IN PLPA

CALLER (where you came from)

IPCS OUTPUT STREAM -----

Command ==> **ip where 084C68B2 reg 14 (from addr)**

***** TOP O

ASID(X'00A2') 084C68B2. **IGG0CLHA+78B2** IN EXTENDED PLPA

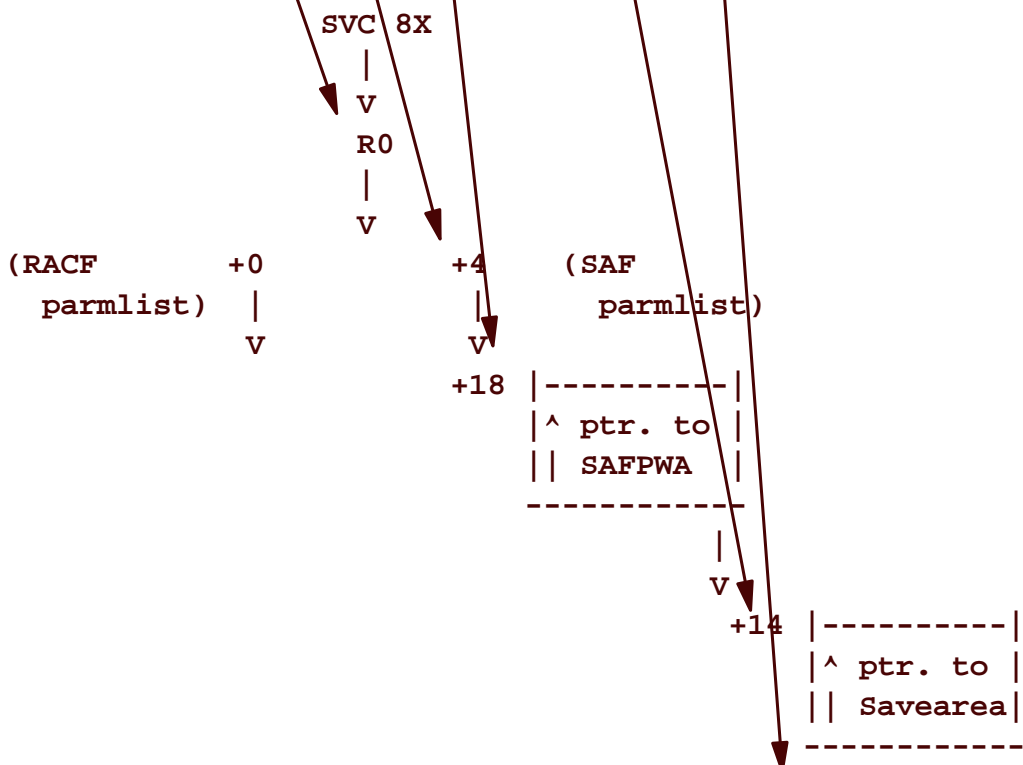
***** END O

Remember, RACROUTE is called via a BALR R14,R15. This invokes SAF router (ICHSFR00) which inturn calls the RACF router (ICHRFR00) to do the actual SVC (x'82', x'83', x'84', x'85') invocation.

Locating the caller of RACROUTE

1 R0+4?+18?+14?+c?-2

This way of finding the caller is to go to the SAF workarea....



	1stword	2ndword	3rdword	4thword	5thword
	+0	+4	+8	+c	+10
In the savearea:	Garbage	HSA	LSA	R14 (caller) Go to Addr. and back up to find module/lvl	R15 (should pt to ICHSFR00 +0 Do IP Where on Addr. in R15. (good to verify you are in the right savearea)



**Still
awake ???**

ICH408I - get the **WHOLE** message

```
ICH408I USER(SMITH ) GROUP(DEPT60 ) NAME(R.L.SMITH )  
ICH408I DEPT58.CLIST.CNTL CL(DATASET ) VOL(TSO035)  
ICH408I INSUFFICIENT ACCESS AUTHORITY  
ICH408I FROM DEPT58.CLIST.* (G)  
ICH408I ACCESS INTENT(READ ) ACCESS ALLOWED(NONE )
```

It tells a story. **WHO, WHAT, and WHY**

Perhaps, most important is the **WHO**.

The "who" should be an identifiable userid / group.

It is important to note if it's JOB() STEP().

Indicates that task is either unidentified (to RACF) or
call was made with token / userid not defined to RACF

In the case of user / token undefined it may be another address spaces call.

Use WTO slip mentioned in previous topic.

```
ICH408I USER(HARDGR3 ) GROUP( ) NAME(???)  
LOGON/JOB INITIATION - USER AT TERMINAL NOT RACF-DEFINED  
IRR012I VERIFICATION FAILED. USER PROFILE NOT FOUND.
```

ICH408I - get the WHOLE message

```
ICH408I USER(HARDGR3 ) GROUP(TSOGRP ) NAME(HARDGR3 ID #3 )  
HARDGRO.DATASET.ONE CL(DATASET ) VOL(UNDETE)  
WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED  
FROM HARDGRO.DATASET.ONE (G)  
ACCESS INTENT(UPDATE ) ACCESS ALLOWED(NONE )
```

```
AUTHCHKI RC EQ 0
```

```
ICH408I USER(HARDGR3 ) GROUP(TSOGRP ) NAME(HARDGR3 ID #3 )  
HARDGRO.DATASET.TWO CL(DATASET ) VOL(UNDETE)  
INSUFFICIENT ACCESS AUTHORITY  
FROM HARDGRO.DATASET.TWO (G)  
ACCESS INTENT(UPDATE ) ACCESS ALLOWED(NONE )
```

```
AUTHCHKI RC EQ 8
```

```
ICH408I USER(HARDGR3 ) GROUP(TSOGRP ) NAME(HARDGR3 ID #3 )  
HARDGRO.DATASET.TRE CL(DATASET ) VOL(UNDETE)  
INSUFFICIENT ACCESS AUTHORITY  
FROM HARDGRO.DATASET.TRE (G)  
ACCESS INTENT(UPDATE ) ACCESS ALLOWED(READ )
```

```
AUTHCHKI RC EQ 8
```

ICH408I - get the WHOLE message

```
ICH408I  JOB(IEESYSAS) STEP(IGG0CLX0)  IXLSTR.SYSIGGCAS_ECS  
CL(FACILITY)  
INSUFFICIENT ACCESS AUTHORITY  
FROM IXLSTR.** (G)  
ACCESS INTENT(ALTER ) ACCESS ALLOWED(NONE )
```

```
ICH408I  JOB(MSTRJCL ) STEP(DUMPSRV )  
IXLSTR.SYSZWLM_WORKUNIT CL(FACILITY)  
INSUFFICIENT ACCESS AUTHORITY  
FROM IXLSTR.** (G)  
ACCESS INTENT(ALTER ) ACCESS ALLOWED(NONE )
```

When the jobname is IEESYSAS, the action (usually) is to define the stepname as the started task name.

The above examples were corrected by defining WLM.

The CALLER vs RACF

- Who is responsible for what?

- Caller's

- parameter list setup
- handling return code

- RACF's

- accurately handling call
- passing info back to caller

- Who actually denies access??

- The caller !!

>>>> (not RACF) <<<<

- Biggest factor is what call was made when (and why).
(multiple calls)

- CATALOG calls RACF several times and suppress many (if not all) messages.

- Best to take up with our caller :-D

APARS of interest October 2003

page 1 of 2

OW52914 SEV3 BUFFER SERIALIZATION PROBLEMS IN RACF DATASHARING

OW54280 SEV3 ABEND878 RUNNING A LISTUSER WITH AN ASTERISK

OW55047 SEV3 ABEND0C1 IN RACF INITIALIZATION WHEN IPLING 2ND LPAR

OW55071 SEV2 RACF REMOTE SHARING CONNECTION REPEATEDLY FAILS

OW56274 SEV2 ABEND0E0 RC29 IN IRRACM00 LEADS TO ABEND0C4 AND
LOSS OF SYSTEM

OW56843 SEV3 PROTECTED USERIDS ARE REVOKED FOR INACTIVITY

OA04924 SEV3 ABENDDD23 IN IRRSSSI2 ISSUING COMMANDS FROM IR

OA02721 SEV2 IN SOME ENVIRONMENTS, PERFORMANCE OF GET_UMAP

OA02850 SEV3 DOCUMENTATION FOR USE OF DYNAMIC GRS RNL CHAN

OA03218 SEV3 SAFTRACE MAY INCORRECTLY FORMAT THE ACEE IN C

OA05119 SEV3 REPLACE EXPIRING CERTIFICATE AUTHORITY DIGITA

OA01560 SEV2 FACILITY PROFILE IRR.PGMSECURITY WITH APPLDAT

OA02038 SEV2 SYSTEM HANG ON RACF LATCH IRRXCF00.LATCHSET.PRIMARY
DUP of OW56383

OA02110 SEV2 WHEN THE RACLIST SELECTION EXIT IS BEING USED

APARS of interest October 2003

page 2 of 2

OA02695 SEV3 THE IRR.PASSWORD.RESET FACILITY PROFILE ALLOW

OA03076 SEV2 MVCL (MOVE LONG) IN IRRMPP00 CAN MOVE LARGE
AREA OF STORAGE AND OVERLY SYSTEM

OA03480 SEV2 ICH420I PROGRAM IRXANCHR CAUSED THE ENVIRONMENT
TO BECOME UNCONTROLLED

OA04163 SEV2 RACF IS PERIODICALLY PURGING THE VLF ACEE CAC

OA04203 SEV3 IRRMIN00 WILL NOT CORRECTLY UPDATE ICB IN CF

OA04679 SEV3 ABEND378 RC24 WHEN RUNNING IRRMIN00 PARM=NEW

OA04792 SEV3 ABENDDD23 IRRCRV11 MSGIRRX0171

OA02573 SEV2 0C4 ABEND IN IRRDSG10 IN A SYSPLEX ENVIROMENT

OA02711 SEV3 PADS-CHECKING UNUSABLE WHEN IDENTIFY USED TO
CREATE A NEW CSECT

OA03861 SEV2 DIGITAL CERTIFICATES GET MARKED NOTRUST GOING

OA03986 SEV2 ICHRIX02 USAGE TO REDRIVE CAUSES STORAGE CREE

OA04369 SEV1 AN INTERLOCK (DEADLY EMBRACE OR ENQUEUE
LOCKOUT (DUP of OW51898)

III2972 INFO APAR for IRRIRA00

Miscellaneous

- **Templates and dynamic parse.**
 - **TEMPLATES - IRRTEMPI from SYSI.MODGEN**
Should match highest level of software using this RACF DB.
 - **DYNAMIC PARSE TABLE SEGMENTS - IRRDPSDS from SYSI.SAMPLIB.**
MUST match software level of running system
 - ◆ Interaction of these can (and does) cause much confusion.
 - ◆ **ICH577E WARNING: BASE SEGMENT OF USER TEMPLATE AT LEVEL template-level DOES NOT CONTAIN FIELD ffffffff.**

Miscellaneous - continued

■ RACF SUBSYSTEM ASID- it's uses

- One of RRSF's major components.
- Use of IRRSEQ00 (R_Admin callable service)

now LDAP is making much use of this.

- APPC PV (persistent verification - use of RACROUTE REQ=SIGNON service).
- SAFTRACE - SET cmd used to start, filter, stop.
- Enables ability to issue RACF commands via an MVS console.

SET and RVARY don't require logon (plus those dealing with RRSF; TARGET, etc). Most other commands do (AU, AD, CO, RDEF, SETR) etc.

- ◆ **Highly recommended to have up and running**

Miscellaneous- continued

- **Emergency ICHRDSNT**

To specify a different DB (or an *) and perhaps shutoff sysplex comm bit

- **D/R practice - a few "what if" scenarios.**

- **primary DB no good at IPL**
- **backup no good at IPL**
- **out of space conditions**
- **database corruption**
- **do you know the RVARY passwords?**

- **When migrating to a new OS, remember**

- **ICHRIN03**
- **ICHRDSNT and ICHRRNG**
- **ICHRRCDE and ICHRFR01**
- **ICHDEX01 (or not)**
- **ICHR_X01/02 (I, C and D)**
- **miscellaneous exits**
- **compare ICH508I message from two IPLs**
- **look for ICH524I / ICH525I as appropriate**

Personnel

RACF level2 - Poughkeepsie NY

- Rory Blackwell
- Bill Garvin
- Russ Hardgrove
- Iain Keddie
- John RealeIII
- Cheri Prendergast (now does ICSF/SSL)

Some questions and [hopefully] answers

- About presentation?
- About service?
- About IBM?
- ????



Session Summary

- SAFTRACE Facility
- Locating the caller of RACF
- ICH408I - get the whole message
- The caller versus RACF
- APARS of interest
- Miscellaneous
- RACF Level2 Personnel
- Some questions and answers



Additional information

- ▶ **z/OS VIR4.0 Security Server RACF Callable Services**
- ▶ **z/OS VIR4.0 Security Server RACF Diagnosis Guide**
- ▶ **z/OS VIR4.0 Security Server RACF Command Language Reference**
- ▶ **z/OS VIR4.0 Security Server RACF Data Areas**
- ▶ **z/OS VIR4.0 Security Server RACF System Programmer's Guide**
- ▶ **z/OS VIR4.0 Security Server RACF Racroute Macro Reference**
- ▶ **z/OS VIR4.0 Security Server RACF Security Administrator's Guide**
- ▶ **z/OS VIR4.0 Security Server RACF Messages and Codes**
- ▶ **z/OS VIR4.0 Security Server RACF Auditor's Guide**



