RACF Level 2 UPDATE

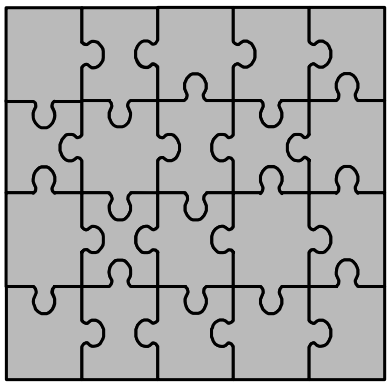
-- a Diagnostic Approach

Vanguard's Enterprise Security

EXPO 2003

July 12-17, 2003

Orlando, Florida



Russ Hardgrove
RACF Level 2 Team Leader
IBM - OS/390 & z/OS Software Service
Poughkeepsie, NY 12601

hardgrov@us.ibm.com


I luv RACF
??????

Agenda

- SAFTRACE Facility
  (z/OS V1R2 -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 V1R2
- 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.
  - R1 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

```
05 00A2 009DD928   SVC    82  070C2000 80DA266E  00000000 00005910 00000000
05 00A2 009DD928   SVC    77  070C2000 88203442  88201FE4 FFF00000 000E0001
05 00A2 009DD928   SVCR   77  070C2000 88203442  00000000 FFF00000 80004000

IPCS OUTPUT STREAM ----------------------------------
Command ===>  ip where 00DA266E
 ************************************************
      ASID(X'00A2') 00DA266E. ICHRFR00+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 ===>  l 00005910
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   | ............... |
```

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

```
  File  Edit  Edit_Settings  Menu  Utilities  Compilers
sssssssssssssssssssssssssssssssssssssssssssssssssssssss
EDIT       RDHARDG.JCL.CNTL(X) - 01.26
Command ===> hex data
005900 ICH408I USER(HARDGR3 )
       C9C3C8F4F0F8C940E4E2C5D94DC8C1D9C4C7D9F3405D4040
       40404040404040404040404040404040404040404040404040
------------------------------------------------------------
****** **************************** Bottom of Data ****
```

```
SLIP DEL,ID=WTO1
SLIP SET,IF,LPAEP=(IGC0003E,0,0),A=SYNCSVCD,ID=WTO1,
 DATA=(1R?+04,EQ,C9C3C8F4,
       1R?+08,EQ,F0F8C940,
       1R?+0C,EQ,E4E2C5D9,
       1R?+10,EQ,4DC8C1D9,
       1R?+14,EQ,C4C7D9F3,
       1R?+14,EQ,405D),
SDATA=(PSA,CSA,LPA,LSQA,RGN,SQA,SUM,SWA,TRT),END
```

(the data parameter is looking for ICH408I USER(HARDGR3) in REG1

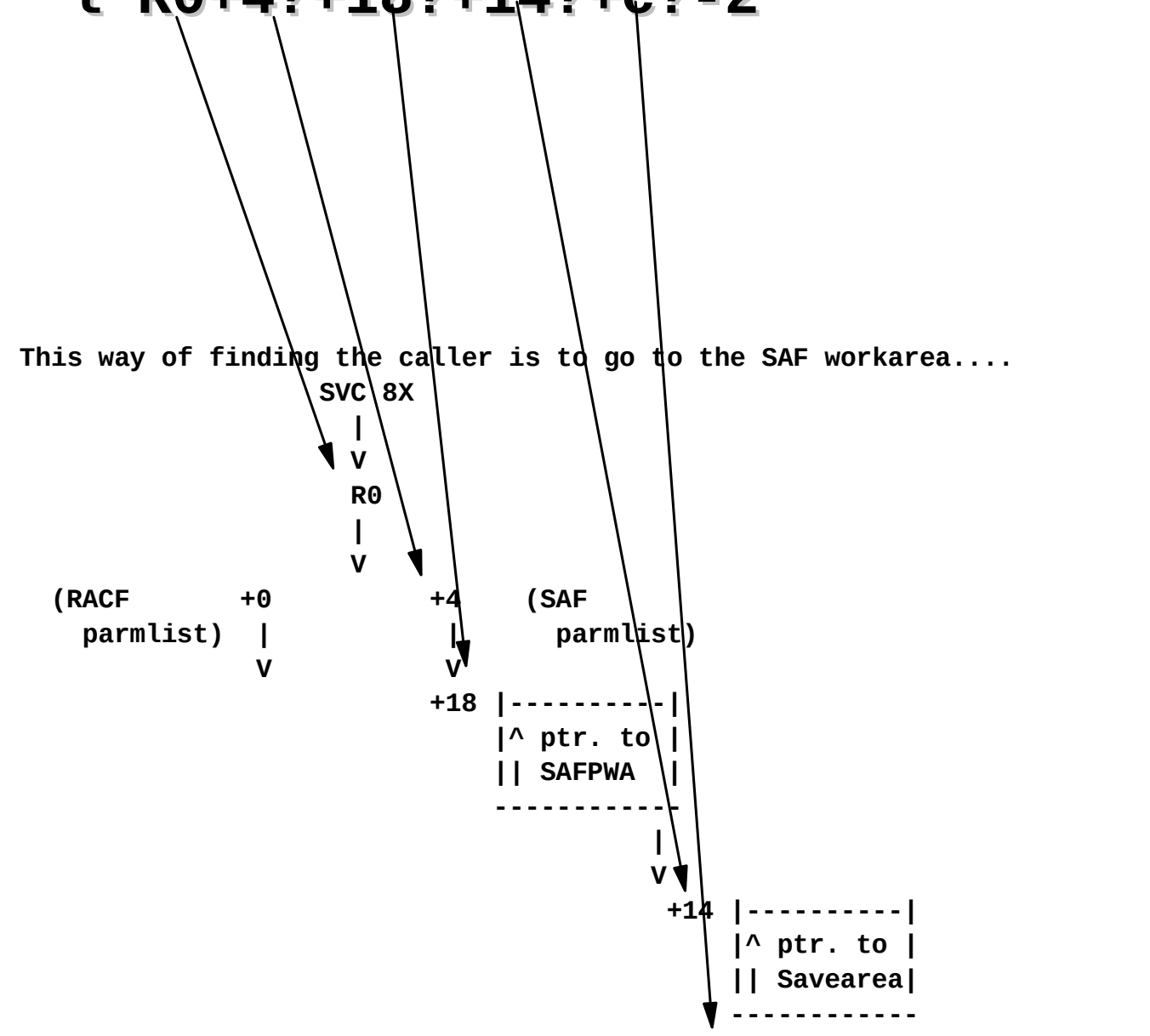
```
ASID(X'001F') ADDRESS(0B200C6C.) STORAGE ----------------------------------
Command ===> l r0+4?+18?+14?+c?-2                    SCROLL ===> C
0B200C6C                                  05EF182F   |             .... |
0B200C70   5830C044   5840C048   182F4170   00044180   | ..{.. {........ |
0B200C80   00081222   4780C1CA   19274780   C1AA1928   | ......A.....A... |

scrolling up to see:

0B200B20   00000000   00000000   90ECD00C   18CF47F0   | ..........}....0 |
0B200B30   C03040C1   E4E3C8C3   C8D2F140   404040E5   | {. AUTHCHK1    V |
0B200B40   F14BF040   40604040   C7D9C9D5   C3C840F0   | 1.0  -  GRINCH 0 |
0B200B50   F761F2F2   61F0F100   50D0C204   41D0C200   | 7/22/01.&}B..}B. |
0B200B60   41500003   4160C448   4510C0AC   00000000   | .&...-D...{..... |
```

Locating the caller of RACROUTE

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



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   )

AUTHCHK1 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   )

AUTHCHK1 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   )

AUTHCHK1 RC EQ 8
```

ICH408I - get the whole message

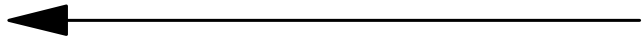
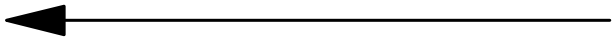
ICH408I **JOB(IEESYSAS) STEP(IGG0CLX0)** IXLSTR.SYSIGGCAS_ECS
CL(FACILITY)
INSUFFICIENT ACCESS AUTHORITY
FROM IXLSTR.** (G)
ACCESS INTENT(ALTER) ACCESS ALLOWED(NONE)

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 July2003

OW51898 SEV3 SYSZRACF2 ENQUEUE LOCKOUT/ SPLIT DB / IRRGTS

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 SECOND LPAR

OW55071 SEV2 RACF REMOTE SHARING CONNECTION REPEATEDLY FAILS

OW55131 SEV2 RRSF ADDRESS SPACE ABENDS AND DOESN'T RECOVER

OW56154 SEV3 SYSTEMS JOINING A RACF GROUP (IRRXCF00) MAY HAVE BKP INACTIVE

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

OW56383 SEV2 SYSTEM HANG ON RACF LATCH IRRXCF00.LATCHSET.PRIMARY

OW56843 SEV3 PROTECTED USERIDS ARE REVOKED FOR INACTIVITY

OA02038 SEV2 SYSTEM HANG ON RACF LATCH IRRXCF00.LATCHSET.PRIMARY

OA02110 SEV2 WHEN THE RACLIST SELECTION EXIT IS BEING USED

OA02573 SEV2 0C4 ABEND IN IRRDSG10 IN A SYSPLEX ENVIROMENT

OA02616 SEV2 RACROUTE REQ=AUTH WITH ENTITY=(XXXXXX,PRIVATE) LEADS TO STROAGE LEAK

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

OA02721 SEV2 IN SOME ENVIRONMENTS, PERFORMANCE OF GET_UMAP

OA02850 SEV3 DOCUMENTATION FOR USE OF DYNAMIC GRS RNL CHAN

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

OA03480 SEV2 ICH420I PROGRAM IRXANCHR CAUSED THE ENVIRONMENT TO BECOME UNCONTROLLED

II12972 INFO APAR for IRRIRA00

Miscellaneous

- Templates and dynamic parse.

  - TEMPLATES - IRRTEMP1 from SYS1.MODGEN
    Should match highest level of software using this RACF DB.
  - DYNAMIC PARSE TABLE SEGMENTS - IRRDPSDS from SYS1.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- 5 Uses

1. **One of RRSF's major components.**
2. **Use of IRRSEQ00 (R_Admin callable service)** now LDAP is making much use of this.
3. **APPC PV (persistant verification - use of RACROUTE REQ=SIGNON service).**
4. **SAFTRACE - SET cmd used to start, filter, stop.**
5. **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 V1R4.0 Security Server RACF Callable Services
- z/OS V1R4.0 Security Server RACF Diagnosis Guide
- z/OS V1R4.0 Security Server RACF Command Language Reference
- z/OS V1R4.0 Security Server RACF Data Areas
- z/OS V1R4.0 Security Server RACF System Programmer's Guide
- z/OS V1R4.0 Security Server RACF Racroute Macro Reference
- z/OS V1R4.0 Security Server RACF Security Administrator's Guide
- z/OS V1R4.0 Security Server RACF Messages and Codes
- z/OS V1R4.0 Security Server RACF Auditor's Guide


Now I really
luv RACF !!!