22 RACF

November 2000

update

In this issue

RACF Update

Published by

Xephon
27-35 London Road
Newbury
Berkshire RG14 1JL
England
Telephone: 01635 38030
From USA: 01144 1635 38030
E-mail: fionah@xephon.com

North American office

Xephon
Post Office Box 350100
Westminster CO 80035-0100
USA
Telephone: (303) 410-9344

RACF Update on-line

You can download code from *RACF Update* from our Web site at http://www.xephon.com/racfupdate.html; you will need the user-id shown on your address label.

Subscriptions and back-issues

A year's subscription to *RACF Update*, comprising four quarterly issues, costs £190.00 in the UK; $290.00 in the USA and Canada; £196.00 in Europe; £202.00 in Australasia and Japan; and £200.50 elsewhere. In all cases the price includes postage. Individual issues, starting with the August 1995 issue, are available separately to subscribers for £50.50 ($77.50) each including postage.

Editor

Fiona Hewitt

Disclaimer

Readers are cautioned that, although the information in this journal is presented in good faith, neither Xephon nor the organizations or individuals that supplied information in this journal give any warranty or make any representations as to the accuracy of the material it contains. Neither Xephon nor the contributing organizations or individuals accept any liability of any kind howsoever arising out of the use of such material. Readers should satisfy themselves as to the correctness and relevance to their circumstances of all advice, information, code, JCL, and other contents of this journal before making any use of it.

Contributions

Articles published in *RACF Update* are paid for at the rate of £170 ($260) per 1000 words and £100 ($160) per 100 lines of code for the first 200 lines of original material. The remaining code is paid for at the rate of £50 ($80) per 100 lines. In addition, there is a flat fee of £30 ($50) per article. To find out more about contributing an article, without any obligation, please contact us at any of the addresses above and we will send you a copy of our *Notes for Contributors*, or you can download a copy from www.xephon.com/contnote.html

Printed in England.

A user SVC for authorized functions

PROBLEM

We wanted functions that could be executed only in an authorized environment (ie APF or supervisor state or key 0) to be available in unauthorized environments (ie not APF and problem state and key 8). That is, to be available in any application program.

We were dealing with RACF retrievals of data with no security issues, so that some, or maybe even all, users should have been able to use it. Despite this, RACF required the caller to be in the authorized state.

SOLUTION

The only general solution to this problem was to develop the SVC presented here. Note that although the functions are currently all RACF retrievals, future functions don't necessarily have to do with RACF, and this SVC can be extended to any functions in a modular way.

Because an SVC can be called directly only from an Assembler program, I developed a program interface to enable it to be called from higher programming languages such as PL/I and COBOL (calling it as an external subroutine, preferable dynamically). It can also be called from CLIST and REXX as a TSO command, in which case the result is returned by means of screen output that can be intercepted if necessary. See below for further details.

INSTALLATION

The installation steps are as follows:

- Define the SVC in SYS1.PARMLIB(IEASVCxx):

  ```
  SVCPARM  255,REPLACE,TYPE(3),EPNAME(USERSVC)
  ```

  In this case, the SVC-number is 255. Choose an unused SVC number.

- Put the chosen SVC number into the program interface module AUTHFNC at the indicated place.
- Install the USERSVC SVC load module in SYS1.LPALIB, and the AUTHFNC program interface load module in SYS1.LINKLIB, preferably as SMP usermod.
- For testing purposes, USERSVC can be assembled as a normal program instead of an SVC. To do this, code

  ```
  PARM.C='...,BATCH,SYSPARM(NOSVC)'
  ```

  in JCL.

  In this case, the program also gets attribute AC(1).
- The functions of the SVC are protected by RACF. All users have to be authorized by RACF for the respective function – give the user READ authority to profile USERSVC.function in class FACILITY. For example:

  ```
  RDEF FACILITY USERSVC.**  UACC(NONE)
  ```

  (prohibit all functions that are not explicitly defined.)

  ```
  RDEF FACILITY USERSVC.LU1 UACC(NONE)
  ```

  (define the LU1 function and prohibit it generally.)

  ```
  PE USERSVC.LU1 CLASS(FACILITY) ID(SYSPROG) ACCESS(READ)
  ```

  (all users of SYSPROG group can execute LU1 function.)

FUNCTIONS

Three functions are shown as examples (marked as functions 1, 4, and 8 in the source program below):

```
 (1) return name field of a RACF user
    parameter | i/o | type | length |
    ----------+-----+------+--------+
    'LU1'     | in  | char |      8 |
    user      | in  | char |      8 |
    name      | out | char |     2Ø |
```

```
    rc | meaning
    ---+-------------------------------------------------------------
     Ø | user exists, name returned
     8 | user doesn't exist
(4) return all entries of the access list for a given data set name
    parameter | i/o | type | length | remarks
    ----------+-----+------+--------+---------------------------------
    'LD1'     | in  | char |      8 |
    dsname    | in  | char |     44 |
    access    | out | char |   1Ø24 | = 64*(8+8) : max 64
              |     |      |        | user/group + authority

    rc | meaning
    ---+-------------------------------------------------------------
     Ø | profile for DSN exists, all access list entries returned
     4 | profile for DSN exists, first 64 access list entries returned
     8 | profile for DSN doesn't exist
 (8) execute RACF TSO command 'SETROPTS LIST'
    (works only in TSO environment)
    parameter | i/o | type | length |
    ----------+-----+------+--------+
    'SETR1'   | in  | char |      8 |

    rc | meaning
    ---+-------------------------------------------------------------
     Ø | execution of TSO command 'SETROPTS LIST' successful
     8 | execution of TSO command 'SETROPTS LIST' failed
    2Ø | not in TSO environment
```

CALLING SEQUENCES

The calling sequences are shown below.

Assembler

```
        .....
         LA    R1,PARM@
         SVC   255
* RETURN CODE IN R15:
*  Ø = FUNCTION OK
*  4 = FUNCTION OK, BUT DATA TRUNCATED (RETURN AREA TOO SMALL)
*  8 = FUNCTION FAILED (EG DATA NOT FOUND)
* 12 = USER NOT AUTHORIZED FOR FUNCTION
* 16 = INVALID FUNCTION OR WRONG ARGUMENT FOR FUNCTION
         LTR   R15,R15
         BZ    OK
         .....
```

```
PARM@    DC    A(PARM1,PARM2,PARM3+X'80000000')
PARM1    DC    CL8'LU1'
PARM2    DC    CL8'USER1'
PARM3    DS    CL20
         .....
```

PL/I

```
.....
 /* AUTHFNC IS PROGRAM INTERFACE TO USER SVC, PASSING ARGUMENTS THE SAME
    WAY */
 DCL AUTHFNC ENTRY OPTIONS(ASM INTER RETCODE);
 FETCH AUTHFNC;
 DCL FNC  CHAR(8) STATIC INIT('LU1');
 DCL USER CHAR(8) STATIC INIT('USER1');
 DCL NAME CHAR(20);
 CALL AUTHFNC(FNC,USER,NAME);
 SELECT (PLIRETV());
   WHEN (0) DISPLAY('NAME OF '||USER||' IS '||NAME);
   WHEN (8) DISPLAY('USER '||USER||' DOESN''T EXIST');
   OTHER    DISPLAY('AUTHFNC: UNEXPECTED RC=',PLIRETV());
 END;
 .....
```

CLIST

```
.....
 /* AUTHFNC IS PROGRAM INTERFACE TO USER SVC, CALLED AS TSO COMMAND:
 /* - INPUT PARAMETER AS CHARACTER STRING BEHIND COMMAND
 /* - RESULT IS SCREEN OUTPUT THAT CAN BE INTERCEPTED
 SET SYSOUTTRAP = 65
 AUTHFNC LD1 A.B.C
 WRITE RC=&LASTCC
 /* ADDITIONAL RETURN CODE WHEN CALLING IT AS TSO COMMAND:
 /* 20 = OUTPUT TO SCREEN FAILED
 SET SYSOUTTRAP = 0
 IF &LASTCC <= 4 THEN DO
   WRITE UACC=&SUBSTR(9:16,&STR(&SYSOUTLINE1))
   DO &I = 2 TO &SYSOUTLINE
     SET S = &STR(&&SYSOUTLINE&I)
     WRITE USER/GRP=&SUBSTR(1:8,&S)  ACCESS=&SUBSTR(9:16,&S)
   END
 END
 .....
```

REXX

```
.....
 V = OUTTRAP('S.')
```

```
ADDRESS TSO "AUTHFNC LD1 A.B.C"
SAY 'RC='RC
V = OUTTRAP('OFF')
IF RC <= 4 THEN DO
  SAY 'UACC='SUBSTR(S.1,9,8)
  DO I = 2 TO S.Ø
    SAY 'USER/GRP='SUBSTR(S.I,1,8)  'ACCESS='SUBSTR(S.I,9,8)
  END
END
.....
```

PROGRAM SOURCE

```
TITLE '------- USERSVC ------- USER SVC -------'
* REGISTER USAGE
*   RØ  : CALLER; WORK
*   R1  : CALLER; WORK
*   R2  : WORK
*   R3  : ADDRESS OF CVT; WORK
*   R4  : ADDRESS OF TCB
*   R5  : ADDRESS OF SVRB
*   R6  : ENTRY ADDRESS; BASE
*   R7  : ADDRESS OF ASCB
*   R8  : WORK
*   R9  : WORK
*   R1Ø : WORK
*   R11 : WORK; ADDRESS OF PARAMETER ADDRESSES
*   R12 : WORK; ADDRESS OF ENTRY IN FUNCTION TABLE
*   R13 : CALLER; ADDRESS OF SAVE AREA
*   R14 : RETURN ADDRESS
*   R15 : CALLER; RETURN CODE
         PRINT NOGEN               MACRO EXPANSION INVISIBLE
         YREGS ,                   REGISTER SYMBOLS
USERSVC  CSECT ,                   PARM.L='REUS,RENT,REFR'
USERSVC  RMODE ANY
USERSVC  AMODE 31
         LCLA  &SUBPOOL
                                                              SPACE
         AIF   ('&SYSPARM' EQ 'NOSVC').SVC1Ø
*                                  ASSEMBLE AS SVC
&SUBPOOL SETA  229
         USING USERSVC,R6
         B     LSTART
         DC    AL1(L'KID)
KID      DC    C'USERSVC  &SYSDATC &SYSTIME '
LSTART   DS    ØH
         LR    R8,R14              CONTENTS OF REGS 14,Ø,1 HAVE TO BE
         LR    R1Ø,RØ                UNCHANGED AT RETURN FROM SVC,
```

```
         LR    R11,R1                THEREFORE SAVE THEM
         LA    RØ,VARSL              LENGTH OF VARIABLE AREA
         STORAGE OBTAIN,LENGTH=(Ø),LOC=ANY,SP=&SUBPOOL
         LR    R13,R1                ADDR OF OWN SAVE AREA = ADDR OF VARS
         USING VARS,R13
         LR    RØ,R1
         LA    R1,VARSL
         XR    R15,R15
         MVCL  RØ,R14                CLEAR VARIABLE AREA
         XR    R9,R9                 RETURN CODE = Ø
         STM   R8,R11,VSAVSVC
         AGO   .SVC2Ø
                                                                SPACE
.SVC1Ø   ANOP  ,
*                                    FOR TEST: ASSEMBLE AS PROGRAM
&SUBPOOL SETA  Ø
         SAVE  (14,12),,'USERSVC  &SYSDATC &SYSTIME '
         LR    R6,R15
         USING USERSVC,R6
         LR    R11,R1                ADDRESS OF PARAMETER ADDRESSES
         LA    RØ,VARSL              LENGTH OF VARIABLE AREA
         STORAGE OBTAIN,LENGTH=(Ø),LOC=ANY,SP=&SUBPOOL
         LR    R2,R1                 SAVE ADDRESS OF VARIABLE AREA
         LR    RØ,R1
         LA    R1,VARSL
         XR    R15,R15
         MVCL  RØ,R14                CLEAR VARIABLE AREA
         ST    R2,8(,R13)            CHAIN SAVE AREAS
         ST    R13,4(,R2)
         LR    R13,R2                ADDR OF OWN SAVE AREA = ADDR OF VARS
         USING VARS,R13
.SVC2Ø   ANOP  ,
                                                              EJECT
*********************************************************************
* DETERMINE REQUESTED FUNCTION, VERIFY PARAMETERS
*********************************************************************
         LTR   R11,R11               NO PARAMETER ?
         BZ    LPARERR                 YES
         L     R1,Ø(,R11)            ADDR OF 1ST PARAMETER = FUNCTION
         CLC   KFKTINT,Ø(R1)         INTERNAL FUNCTION ?
         BNE   LP1                     NO
         L     R1,4(,R11)            FUNCTION AS 2ND PARAMETER
LP1      DS    ØH
                                                              SPACE
         LA    R12,KFKTTAB-DFKTTABL  ADDR ØTH ENTRY IN FUNCTION TABLE
         USING DFKTTAB,R12
         LA    R14,DFKTTABL          INCREMENT = LENGTH OF A TABLE ENTRY
         LA    R15,KFKTTABX-DFKTTABL  ADDR OF LAST ENTRY IN FUNC TABLE
LP1LOOP  DS    ØH
         BXLE  R12,R14,LP1CMP        TO NEXT TABLE ENTRY
```

```
         B     LPARERR             FUNCTION UNKNOWN
LP1CMP   DS    ØH
         CLC   DFKT,Ø(R1)          FUNCTION FOUND ?
         BNE   LP1LOOP               NO
                                                        SPACE
         L     R1,Ø(,R11)          ADDR OF 1ST PARAMETER = FUNCTION
         CLC   KFKTINT,Ø(R1)       INTERNAL FUNCTION ?
         BNE   LP1X                  NO
         LA    R15,DNPARM          RETURN ADDRESS OF ENTRY IN FUNCTION
         ST    R15,VRCF              TABLE FOR PARAMETER
         B     LRETURN
LP1X     DS    ØH
                                                        SPACE
         LR    R1,R11              ADDRESS OF 1ST PARAMETER ADDRESS
         LA    R14,4               INCREMENT = LENGTH OF A PAR ADDRESS
         XR    R15,R15
         IC    R15,DNPARM          EXPECTED PARAMETER COUNT
         BCTR  R15,Ø               - 1
         SLL   R15,2               * 4
         ALR   R15,R1              ADDRESS OF LAST EXPECTED PAR ADDRESS
LP@LOOP  DS    ØH
         TM    Ø(R1),X'8Ø'         LAST PARAMETER ADDRESS ?
         BO    LP@LAST               YES
         BXLE  R1,R14,LP@LOOP
         B     LPARERR             TOO MANY PARS OR LAST ADDR NOT X'8Ø'
LP@LAST  DS    ØH
         CLR   R1,R15              LAST PAR AT EXPECTED POSITION ?
         BNE   LPARERR               NO, TOO FEW PARAMETERS
                                                        SPACE
         MVC   VRACRA,KRACRA       RACROUTE PARAMETER LIST
         LA    R1,L'VPROFIL1+L'VPROFIL2  MAX LENGTH OF PROFILE
         STH   R1,VPROFILL
         MVC   VPROFIL1,KPROFIL1   1ST PART OF PROFILE
         MVC   VPROFIL2,DFKT       2ND PART OF PROFILE = FUNCTION
         RACROUTE REQUEST=AUTH,    CHECK AUTHORIZATION FOR FUNCTION    +
               ATTR=READ,                                              +
               CLASS=KCLASS,                                           +
               ENTITYX=VPROFIL,                                        +
               RELEASE=1.9,                                            +
               WORKA=VSAFWRK,                                          +
               MF=(E,VRACRA)
         LA    RØ,4
         CLR   R15,RØ              USER AUTHORIZED ?
         BH    LSECERR               NO
                                                        SPACE
         XR    R15,R15
         ICM   R15,B'ØØØ1',DPARMAI POSITION OF OUTPUT PARAMETER
         BZ    LAPX                ZERO, NO OUTPUT PARAMETER
         BCTR  R15,Ø               - 1
         SLL   R15,2               * 4
```

```
         L     R1,Ø(R15,R11)       ADDRESS OF OUTPUT PARAMETER
         LA    RØ,Ø(,R1)           WITHOUT AMODE BIT
         ST    RØ,VAPARM@          SAVE
         L     R1,DPARMAL          LENGTH OF OUTPUT PARAMETER
         XR    R14,R14
         IC    R15,DPARMAC         PAD CHARACTER
         SLL   R15,24
         MVCL  RØ,R14              PRESET OUTPUT PARAMETER
LAPX     DS    ØH
                                                        SPACE
         L     R15,DGOTO           ADDRESS OF CODE FOR FUNCTION
         BR    R15
LFKTUNV  DS    ØH                  FUNCTION OK BUT DATA INCOMPLETE
         MVI   VRC,4                 (RETURN FIELD TOO SHORT)
         B     LRETURN
LFKTERR  DS    ØH                  FUNCTION FAILED
         MVI   VRC,8                 (EG DATA NOT FOUND)
         B     LRETURN
LSECERR  DS    ØH                  USER NOT AUTHORIZED FOR FUNCTION
         MVI   VRC,12
         B     LRETURN
LPARERR  DS    ØH                  INVALID FUNC OR WRONG PAR FOR FUNC
         MVI   VRC,16
         B     LRETURN
                                                        EJECT
*********************************************************************
* FUNCTION 1
*********************************************************************
L1START  DS    ØH
         MVC   V1RACRX,K1RACRX     RACROUTE PARAMETER LIST
         L     R1,4(,R11)          ADDRESS OF 2ND PARAMETER = USER
         MVC   V1PROFIL,Ø(R1)      RACF PROFILE
         RACROUTE REQUEST=EXTRACT, EXTRACT PROFILE                  +
               TYPE=EXTRACT,                                        +
               CLASS=K1CLASS,                                       +
               ENTITY=V1PROFIL,                                     +
               FIELDS=K1FELD,                                       +
               RELEASE=1.9,                                         +
               WORKA=V1SAFWRK,                                      +
               MF=(E,V1RACRX)
         LTR   R15,R15             PROFILE FOUND ?
         BNZ   LFKTERR               NO
                                                        SPACE
         USING EXTWKEA,R1          ADDRESS RESULT AREA
         LA    R1Ø,LFKTERR         ASSUMING FUNCTION FAILED
         XR    R8,R8
         ICM   R8,B'ØØ11',EXTWOFF  OFFSET OF FIELDS RETURNED
         BZ    L1FREE              NO FIELD RETURNED
         ALR   R8,R1               ADDRESS OF FIELDS RETURNED
         ICM   R9,B'1111',Ø(R8)    LENGTH OF USER'S NAME
```

```
         BZ    L1FREE              NO USER'S NAME
         LA    R1Ø,LRETURN         FUNCTION OK
         L     R2,VAPARM@          ADDRESS OF OUTPUT PARAMETER
         BCTR  R9,Ø
         EX    R9,X1MVC            RETURN USER'S NAME
                                                          SPACE
L1FREE   DS    ØH
         XR    RØ,RØ
         ICM   RØ,B'Ø111',EXTWLN   LENGTH OF RESULT AREA
         XR    R15,R15
         IC    R15,EXTWSP          SUBPOOL OF RESULT AREA
         DROP  R1
         STORAGE RELEASE,LENGTH=(Ø),ADDR=(1),SP=(15)  FREE RESULT AREA
         BR    R1Ø
                                                          EJECT
*********************************************************************
* FUNCTION 4
*********************************************************************
L4START  DS    ØH
         MVC   V4RACRX,K4RACRX     RACROUTE PARAMETER LIST
         L     R1,4(,R11)          ADDRESS OF 2ND PARAMETER = DSNAME
         MVC   V4PROFIL,Ø(R1)      RACF PROFILE
         RACROUTE REQUEST=EXTRACT, EXTRACT PROFILE                  +
               TYPE=EXTRACT,                                        +
               CLASS=K4CLASS,                                       +
               ENTITY=V4PROFIL,                                     +
               FIELDS=K4FELD,                                       +
               RELEASE=1.9,                                         +
               WORKA=V4SAFWRK,                                      +
               MF=(E,V4RACRX)
         LTR   R15,R15             PROFILE FOUND ?
         BNZ   LFKTERR               NO
                                                          SPACE
         USING EXTWKEA,R1          ADDRESS RESULT AREA
         LA    R1Ø,LFKTERR         ASSUMING FUNCTION FAILED
         XR    R8,R8
         ICM   R8,B'ØØ11',EXTWOFF  OFFSET OF FIELDS RETURNED
         BZ    L4FREE              NO FIELD RETURNED
         ALR   R8,R1               ADDRESS OF FIELDS RETURNED
         ICM   R9,B'1111',Ø(R8)    LENGTH OF UACC
         BZ    L4FREE              NO UACC
                                                          SPACE
         L     R2,VAPARM@          ADDRESS OF OUTPUT PARAMETER
         MVC   Ø(L'K4UACC,R2),K4UACC  ID FOR UACC
         XR    RØ,RØ
         IC    RØ,4(,R8)           ACCESS LEVEL BIT
         LA    R3,K4ACCTAB         ADDRESS OF TABLE OF ACCESS LEVELS
L4UACCLO DS    ØH
         SRA   RØ,1                RIGHTMOST BIT SET ?
         BZ    L4UACC                YES
```

```
         LA    R3,8(,R3)           ADDRESS OF NEXT TABLE ENTRY
         B     L4UACCLO
L4UACC   DS    ØH
         MVC   8(8,R2),Ø(R3)       RETURN ACCESS LEVEL
                                                          SPACE
         LA    R1Ø,LRETURN         FUNC OK (MAYBE ACCESS LIST EMPTY)
         LA    R8,4(R9,R8)         ADDRESS OF BYTE BEHIND UACC
         ICM   R9,B'1111',Ø(R8)    TOTAL LENGTH OF ALL FIELDS
         BZ    L4FREE              NO USERS OR GROUPS
                                                          SPACE
         L     R2,VAPARM@          ADDRESS OF OUTPUT PARAMETER
         L     R14,DPARMAL         LENGTH OF OUTPUT PARAMETER
         ALR   R14,R2              ADDRESS OF BYTE BEHIND OUTPUT PAR
         XR    RØ,RØ
         IC    RØ,DPARMA1L         LENGTH OF ONE VALUE IN OUTPUT PAR
         ALR   R2,RØ               ADDRESS OF OUTPUT PAR BEHIND UACC
         LA    R8,4(,R8)           ADDRESS OF 1ST FIELD
         LA    R15,Ø(R9,R8)        ADDRESS OF BYTE BEHIND LAST FIELD
L4LOOP   DS    ØH
         L     R9,Ø(,R8)           LENGTH OF FIELD (USER OR GROUP)
         BCTR  R9,Ø
         EX    R9,X4MVC            RETURN USER OR GRP FROM ACCESS LIST
                                                          SPACE
         XR    RØ,RØ
         IC    RØ,4+4+1(R9,R8)     ACCESS LEVEL BIT
         LA    R3,K4ACCTAB         ADDRESS OF TABLE OF ACCESS LEVELS
L4ACLOOP DS    ØH
         SRA   RØ,1                RIGHTMOST BIT SET ?
         BZ    L4ACC                 YES
         LA    R3,8(,R3)           ADDRESS OF NEXT TABLE ENTRY
         B     L4ACLOOP
L4ACC    DS    ØH
         MVC   8(8,R2),Ø(R3)       RETURN ACCESS LEVEL
                                                          SPACE
         AL    R9,4+1(R9,R8)       PLUS LENGTH OF FIELD (ACCESS BITS)
         LA    R8,4+4+1(R9,R8)     ADDRESS OF NEXT FIELD
         CLR   R8,R15              BEHIND LAST FIELD ?
         BNL   L4FREE                YES
         XR    RØ,RØ
         IC    RØ,DPARMA1L         LENGTH OF ONE VALUE IN OUTPUT PAR
         ALR   R2,RØ               ADDRESS OF NEXT OUTPUT
         CLR   R2,R14              BEHIND OUTPUT PARAMETER ?
         BL    L4LOOP                NO
         LA    R1Ø,LFKTUNV         DATA INCOMPLETE
                                                          SPACE
         B     L4FREE
L4FREE   EQU   L1FREE              REMOVE RESULT AREA
         DROP  R1
                                                          EJECT
```

```
*********************************************************************
* FUNCTION 8
*********************************************************************
L8START  DS    ØH
         USING CVT,R3
         USING TCB,R4
         USING ASCB,R7
         ICM   R9,B'1111',TCBSENV  ADDRESS OF ACEE IN TCB ?
         BNZ   L8ACEE               YES
         L     R8,ASCBASXB         ADDRESS OF ASXB
         USING ASXB,R8
         L     R9,ASXBSENV         ADDRESS OF ACEE
L8ACEE   DS    ØH
         USING ACEE,R9
         L     R1Ø,CVTTVT          ADDRESS OF TSVT
         USING TSVT,R1Ø
                                                          SPACE
         LA    RØ,V8VARSL          LENGTH OF VARIABLE AREA FOR TSOLNK
         STORAGE OBTAIN,LENGTH=(Ø),LOC=ANY,SP=Ø  HAS TO BE SUBPOOL Ø
         LR    R5,R1                               INSTEAD OF 229
         USING V8VARS,R5
         L     R15,TSVTASF         ADDRESS OF MODULE TSOLNK
                                                          SPACE
         MVC   V8ACEEF,ACEEFLG1    AUDITOR ATTRIBUTE FROM ACEE
         OI    V8ACEEF,255-ACEEAUDT  SAVE IT
         OI    ACEEFLG1,ACEEAUDT   MAKE USER TEMPORARILY AN AUDITOR
         CALL  (15),(K8TSOP1,K8TSOP2,K8TSOP3,V8TSOP4,V8TSOP5,V8TSOP6), +
               VL,MF=(E,V8CALL)    CALL TSO COMMAND 'SETROPTS LIST'
         NC    ACEEFLG1,V8ACEEF    AUDITOR ATTRIBUTE AS IT HAS BEEN
                                                          SPACE
         ST    R15,V8RC            SAVE RC
         MVC   V8TSOP5X,V8TSOP5    POSSIBLY REASON CODE, SAVE IT
         DROP  R5
         LR    R1,R5               ADDRESS OF VARIABLE AREA FOR TSOLNK
         LA    RØ,V8VARSL          LENGTH OF VARIABLE AREA FOR TSOLNK
         STORAGE RELEASE,LENGTH=(Ø),ADDR=(1),SP=Ø
                                                          SPACE
         ICM   R15,B'1111',V8RC    COMMAND OK ?
         BZ    LRETURN              YES
         LA    RØ,12               4 = RC>Ø, 8 = ATTENTION, 12 = ABEND
         CLR   R15,RØ              TSO COMMAND FAILED ?
         BNH   LFKTERR              YES
         LA    RØ,2Ø
         CLR   R15,RØ              NOT TSO ENVIRONMENT ?
         BNE   L8ABEND              NO, ANY OTHER ERROR
         LA    RØ,24
         CL    RØ,V8TSOP5X         NOT TSO ENVIRONMENT ?
         BNE   L8ABEND              NO, ANY OTHER ERROR
         MVI   VRC,2Ø              RC: NOT IN TSO ENVIRONMENT
         B     LRETURN
```

```
L8ABEND  DS    ØH                  ANY OTHER ERROR, SHOULD NOT OCCUR
         ABEND 999,DUMP
         DROP  R3,R4,R7,R8,R9,R1Ø
                                                                   EJECT
*********************************************************************
* FINISH
*********************************************************************
LRETURN  DS    ØH
                                                                   SPACE
         AIF   ('&SYSPARM' EQ 'NOSVC').SVC5Ø
*                                  ASSEMBLE AS SVC
         LM    R8,R11,VSAVSVC
         LR    R1,R13               ADDRESS OF VARIABLE AREA
         LA    RØ,VARSL             LENGTH OF VARIABLE AREA
         STORAGE RELEASE,LENGTH=(Ø),ADDR=(1),SP=&SUBPOOL
         LR    R14,R8               RETURN ADDRESS
         LR    R15,R9               RETURN CODE
         LR    RØ,R1Ø               RØ UNCHANGED
         LR    R1,R11               R1 UNCHANGED
         BR    R14                  RETURN, R14 UNCHANGED
         AGO   .SVC6Ø
                                                                   SPACE
.SVC5Ø   ANOP  ,
*                                  FOR TEST: ASSEMBLE AS PROGRAM
         L     R9,VRCF              RETURN CODE
         LR    R1,R13               ADDRESS OF VARIABLE AREA
         L     R13,4(,R13)          AGAIN R13 ADDR OF CALLER'S SAVE AREA
         LA    RØ,VARSL             LENGTH OF VARIABLE AREA
         STORAGE RELEASE,LENGTH=(Ø),ADDR=(1),SP=&SUBPOOL
         LR    R15,R9               RETURN CODE
         RETURN (14,12),,RC=(15)
.SVC6Ø   ANOP  ,
                                                                   EJECT
*********************************************************************
* CONSTANTS
*********************************************************************
KFKTTAB  DS    ØF                   TABLE OF FUNCTIONS
         DC    CL8'LU1     ',A(L1START),AL1(3,3,C' ',2Ø),A(2Ø*ØØØ1)
         DC    CL8'LD1     ',A(L4START),AL1(3,3,C' ',16),A(16*1ØØØ)
         DC    CL8'SETR1   ',A(L8START),AL1(1,Ø,ØØØØ,ØØ),A(ØØ*ØØØØ)
KFKTTABX DS    ØF
KFKTINT  DS    ØXL8                 ID FOR INTERNAL FUNCTION
         DC    7X'FF',X'ØØ'
KPROFIL1 DC    C'USERSVC.'          1ST PART OF PROFILE FOR AUTH CHECK
                                                                   SPACE
KRACRA   RACROUTE REQUEST=AUTH,     RACROUTE PARAMETER LIST PROTOTYPE   +
               RELEASE=1.9,                                            +
               MF=L
KRACRAL  EQU   *-KRACRA             LENGTH OF RACROUTE PARAMETER LIST
KCLASS   DC    AL1(8)               REQ=AUTH: LENGTH IN FRONT OF CLASS,
```

```
         DC    CL8'FACILITY'         REQ=EXTRACT: WITHOUT LENGTH!!!
                                                                SPACE
KRACRX   RACROUTE REQUEST=EXTRACT, RACROUTE PARAMETER LIST PROTOTYPE   +
               TYPE=EXTRACT,                                          +
               GENERIC=YES,                                           +
               MATCHGN=YES,                                           +
               RELEASE=1.9,                                           +
               SUBPOOL=&SUBPOOL,                                      +
               MF=L
KRACRXL  EQU   *-KRACRX            LENGTH OF RACROUTE PARAMETER LIST
                                                                SPACE 3
*************************************************************************
* CONSTANTS FOR FUNCTION 1
*************************************************************************
X1MVC    MVC   Ø(1,R2),4(R8)       RETURN USER'S NAME
K1RACRX  EQU   KRACRX              RACROUTE PARAMETER LIST PROTOTYPE
K1RACRXL EQU   KRACRXL             LENGTH OF RACROUTE PARAMETER LIST
K1CLASS  DC    CL8'USER'           RACF CLASS FOR RACROUTE
K1FELD   DC    A(1)                NUMBER OF FIELDS TO GET FROM PROFILE
         DC    CL8'PGMRNAME'       FIELD FROM PROFILE: USER'S NAME
                                                                SPACE 3
*************************************************************************
* CONSTANTS FOR FUNCTION 4
*************************************************************************
X4MVC    EQU   X1MVC               RETURN USER OR GROUP
K4RACRX  EQU   KRACRX              RACROUTE PARAMETER LIST PROTOTYPE
K4RACRXL EQU   KRACRXL             LENGTH OF RACROUTE PARAMETER LIST
K4CLASS  DC    CL8'DATASET'        RACF CLASS FOR RACROUTE
K4FELD   DC    A(2)                NUMBER OF FIELDS TO GET FROM PROFILE
         DC    CL8'UNIVACS'        FIELD FROM PROFILE: UACC
         DC    CL8'ACL1'           FIELD FROM PROF: USER/GRP + ACC LVL
K4ACCTAB DS    ØCL(8*8)            TABLE OF ACCESS LEVELS
K4ANONE  DC    CL8'NONE    '       CORRESPONDS TO B'ØØØØØØØ1'
         DC    CL8'********'       CORRESPONDS TO B'ØØØØØØ1Ø' (UNUSED)
         DC    CL8'********'       CORRESPONDS TO B'ØØØØØ1ØØ' (UNUSED)
         DC    CL8'EXECUTE '       CORRESPONDS TO B'ØØØØ1ØØØ'
K4AREAD  DC    CL8'READ    '       CORRESPONDS TO B'ØØØ1ØØØØ'
         DC    CL8'UPDATE  '       CORRESPONDS TO B'ØØ1ØØØØØ'
         DC    CL8'CONTROL '       CORRESPONDS TO B'Ø1ØØØØØØ'
         DC    CL8'ALTER   '       CORRESPONDS TO B'1ØØØØØØØ'
K4UACC   DC    C'UACC='            ID FOR UACC IN 1ST OUTPUT FIELD
                                                                SPACE 3
*************************************************************************
* CONSTANTS FOR FUNCTION 8
*************************************************************************
K8TSOP1  DS    ØF                  1ST PARAMETER FOR TSOLNK: FLAGS
         DC    X'ØØ'               ALWAYS ZERO
         DC    X'ØØ'               ISOLATED ENVIRONMENT BECAUSE OF APF
         DC    X'Ø1'               DUMP IN CASE OF ABEND
         DC    X'Ø5'               EXECUTE TSO KOMMANDO
```

```
K8TSOP2  DC    C'SETROPTS LIST'    2ND PAR FOR TSOLNK: TSO COMMAND
K8TSOP3  DC    A(L'K8TSOP2)        3RD PAR FOR TSOLNK: LENGTH OF CMD
                                                          SPACE 3
*************************************************************************
* END OF CONSTANTS
*************************************************************************
         LTORG ,
         DROP  R13,R12,R6          PERMANENT REGISTERS
                                                          EJECT
*************************************************************************
* VARIABLES
*************************************************************************
* NOTE: BECAUSE R13 IS ALSO BASE REGISTER OF VARIABLE AREA,
*       SAVE AREA HAS TO BE LOCATED AT START OF VARIABLE AREA
VARS     DSECT ,                   VARIABLE AREA
         DS    18F                 OWN SAVE AREA
                                                          SPACE
VSAVSVC  DS    4F                  R14..R1 AT TIME OF CALLING THE SVC
VRC      EQU   VSAVSVC+4+3,1       RETURN CODE
VRCF     EQU   VSAVSVC+4,4
VAPARM@  DS    A                   ADDRESS OF OUTPUT PARAMETER
         DS    ØF
VSAFWRK  DS    XL(SAFWLEN)         SAF WORK AREA
         DS    ØF
VRACRA   DS    XL(KRACRAL)         RACROUTE REQ=AUTH PARAMETER LIST
VPROFIL  DS    ØF                  PROFILE FOR AUTHORIZATION CHECK
VPROFILL DS    H                   MAX LENGTH OF PROFILE
         DS    H                   ZERO
VPROFIL1 DS    CL(L'KPROFIL1)      'USERSVC.'
VPROFIL2 DS    CL8                 FUNCTION
                                                          SPACE
VFKTØ    DS    ØD                  VARS FOR FUNCTIONS STARTING HERE
                                                          SPACE 3
*************************************************************************
* VARIABLES FOR FUNCTION 1
*************************************************************************
         ORG   VFKTØ               OVERLAY VARIABLES OF ALL FUNCTIONS
         DS    ØF
V1SAFWRK DS    XL(SAFWLEN)         SAF WORK AREA
         DS    ØF
V1RACRX  DS    XL(K1RACRXL)        RACROUTE REQ=EXTRACT PARAMETER LIST
V1PROFIL DS    CL8                 PROFILE FOR RACROUTE
                                                          SPACE 3
*************************************************************************
* VARIABLES FOR FUNCTION 4
*************************************************************************
         ORG   VFKTØ               OVERLAY VARIABLES OF ALL FUNCTIONS
         DS    ØF
V4SAFWRK DS    XL(SAFWLEN)         SAF WORK AREA
         DS    ØF
```

```
V4RACRX  DS    XL(K4RACRXL)        RACROUTE REQ=EXTRACT PARAMETER LIST
V4PROFIL DS    CL44                PROFILE FOR RACROUTE
                                                                SPACE 3
*********************************************************************
* VARIABLES FOR FUNCTION 8
*********************************************************************
         ORG   VFKTØ               OVERLAY VARIABLES OF ALL FUNCTIONS
V8RC     DS    F                   RC OF TSOLNK
V8TSOP5X DS    F                   COPY OF 5TH TSOLNK PAR: REASON CODE
V8ACEEF  DS    B                   TO SAVE AUDITOR ATTRIBUTE FROM ACEE
                                                                SPACE
V8VARS   DSECT ,                   VAR AREA FOR TSOLNK IN SUBPOOL Ø
V8CALL   CALL  ,(1,2,3,4,5,6),VL,MF=L  PARAMETER LIST FOR TSOLNK
V8TSOP4  DS    F                   4TH PAR FOR TSOLNK: RC OF COMMAND
V8TSOP5  DS    F                   5TH PAR FOR TSOLNK: REASON CODE
V8TSOP6  DS    F                   6TH PAR FOR TSOLNK: ABEND CODE
         DS    ØD
V8VARSL  EQU   *-V8VARS            LENGTH OF VAR AREA FOR TSOLNK
                                                                SPACE
VARS     DSECT ,                   RESUME DSECT OF VARIABLE AREA
                                                                SPACE 3
*********************************************************************
* END OF VARIABLES
*********************************************************************
         ORG   ,                   BEHIND LONGEST VAR AREA OF A FUNC
         DS    ØD
VARSL    EQU   *-VARS              LENGTH OF VARIABLE AREA
                                                                EJECT
*********************************************************************
* DSECTS
*********************************************************************
DFKTTAB  DSECT ,                   ENTRY IN TABLE OF FUNCTIONS
DFKT     DS    CL8                 FUNCTION
DGOTO    DS    A                   ADDRESS OF CODE FOR FUNCTION
DNPARM   DS    AL1                 PARAMETER COUNT OF FUNCTION
DPARMAI  DS    AL1                 POSITION OF OUTPUT PAR (Ø = NONE)
DPARMAC  DS    C                   CHARACTER TO INITIALIZE OUTPUT PAR
DPARMA1L DS    AL1                 LENGTH OF ONE OUTPUT PARAMETER VALUE
DPARMAL  DS    F                   TOTAL LENGTH OF OUTPUT PARAMETER
DFKTTABL EQU   *-DFKTTAB           LENGTH OF A TABLE ENTRY
                                                                SPACE 3
         ICHSAFW ,                 SAF WORK AREA
                                                                SPACE 3
         ICHSAFP ,                 SAF ROUTER PARAMETER LIST
                                                                SPACE 3
         IRRPRXTW ,                RACROUTE REQ=EXTRACT RESULT AREA
* FOR FORMAT OF DATA RETURNED SEE MANUAL
* RACROUTE MACRO REFERENCE, SECTION RACROUTE REQUEST=EXTRACT
                                                                SPACE 3
```

```
*********************************************************************
* DSECTS FOR FUNCTION 8
*********************************************************************
         IKJTCB ,                  TCB, POSSIBLY POINTING TO ACEE
                                                              SPACE 3
         IHAASCB LIST=NO           ASCB, POINTING TO ASXB
                                                              SPACE 3
         IHAASXB LIST=NO           ASXB, POINTING TO ACEE
                                                              SPACE 3
         IHAACEE ,                 ACEE, CONTAINS AUDITOR BIT
                                                              SPACE 3
         CVT   DSECT=YES           CVT, POINTING TO TSVT
                                                              SPACE 3
         IKJTSVT ,                 TSVT, CONTAINS ADDR OF MODULE TSOLNK
                                                              SPACE 3
*********************************************************************
* END OF DSECTS
*********************************************************************
         END   USERSVC
         AIF   ('&SYSPARM' NE 'NOSVC').SVC9Ø
         PUNCH '   SETCODE AC(1)'  IF PROGRAM INSTEAD OF SVC THEN APF
.SVC9Ø   ANOP  ,
         END   ,
/*
         TITLE '------- AUTHFNC ------- PROGRAM INTERFACE TO USER SVC'
* REGISTER USAGE
*   RØ  : WORK
*   R1  : ADDRESS OF PARAMETER ADDRESS LIST
*   R2  : WORK
*   R3  : WORK
*   R4  : WORK
*   R5  : WORK
*   R6  : WORK
*   R7  : WORK
*   R8  : ADDRESS OF PARAMETER STRING
*   R9  : LENGTH OF PARAMETER STRING
*   R1Ø : ADDRESS OF ENTRY IN FUNCTION TABLE IN SVC
*   R11 : WORK; ADDRESS OF PARAMETER ADDRESS LIST
*   R12 : BASE
*   R13 : ADDRESS OF SAVE AREA; BASE OF VARIABLE AREA
*   R14 : RETURN ADDRESS
*   R15 : ENTRY ADDRESS; RETURN CODE
         PRINT NOGEN,DATA          MACRO EXPANSION INVISIBLE
         YREGS ,                   REGISTER SYMBOLS
AUTHFNC  CSECT ,                   PARM.C='BATCH',
AUTHFNC  RMODE ANY                   PARM.L='REUS,RENT,REFR'
AUTHFNC  AMODE 31
         LCLC  &SVCNR
&SVCNR   SETC  '255'               <=== USER SVC # IN YOUR SHOP ===
```

```
         SAVE  (14,12),,'AUTHFNC  &SYSDATC &SYSTIME SVCNR=&SVCNR '
         USING AUTHFNC,R15
                                                                SPACE
* IF 4 PARAMETERS THEN POSSIBLY IT'S A TSO COMMAND (R1->CPPL),
* BUT THE LEFTMOST BIT OF THE 4TH PARAMETER'S ADDRESS ISN'T SET;
* 3RD PARAMETER IS PSCB, VERIFY IT
         USING CPPL,R1
         LTR   R3,R1               ADDRESS OF PARAMETER ADDRESSES
         BZ    LSUBRTN               ZERO, NOT A TSO COMMAND
         LA    R4,4                INCREMENT VALUE: LENGTH OF AN ADDR
         LA    R5,CPPLECT          ADDRESS OF LAST ADDRESS IN CPPL
LPALOOP  DS    ØH
         TM    Ø(R3),X'8Ø'         LAST PARAMETER ADDRESS ?
         BO    LSUBRTN               YES, NOT A TSO COMMAND
         BXLE  R3,R4,LPALOOP
                                                                SPACE
         USING PSA,Ø
         L     R11,PSATOLD         ADDRESS OF TCB
         USING TCB,R11
         L     R1Ø,TCBJSCB         ADDRESS OF JSCB
         SLL   R1Ø,8
         SRL   R1Ø,8               IT IS A 24 BIT ADDRESS
         USING IEZJSCB,R1Ø
         CLC   JSCBPSCB,CPPLPSCB   PSCB AS 3RD PARAMETER ?
         BE    LTSOCMD               YES, CALLED AS TSO COMMAND
                                                                SPACE
         DROP  R1,Ø,R11,R1Ø
LSUBRTN  DS    ØH                  CALLED AS SUBROUTINE
         RETURN (14,12),,RC=(15)
         ORG   *-2
         AIF   ('&SYSPARM' NE 'NOSVC').SVC1Ø
         USING PSA,Ø
         L     R3,FLCCVT           ADDRESS OF CVT
         L     R4,PSATOLD          ADDRESS OF TCB
         XR    R5,R5               ADDRESS OF SVRB WE HAVEN'T GOT
         L     R7,PSAAOLD          ADDRESS OF ASCB
         DROP  Ø
         XCTL  EP=WRTUSVC
         AGO   .SVC11
.SVC1Ø   ANOP  ,
         SVC   &SVCNR              SVC DOESN'T CHANGE ANY REGISTERS
         BR    R14                   EXCEPT RETURN CODE IN R15
.SVC11   ANOP  ,
         DROP  R15
                                                                SPACE
LTSOCMD  DS    ØH                  CALLED AS TSO COMMAND
         LR    R12,R15
         USING AUTHFNC,R12
         LR    R11,R1              ADDRESS OF PARAMETER ADDRESSES
         USING CPPL,R11
```

```
         LA    RØ,VARSL            LENGTH OF VARIABLE AREA
         STORAGE OBTAIN,LENGTH=(Ø),LOC=ANY
         LR    R2,R1               SAVE ADDRESS OF VARIABLE AREA
         LR    RØ,R1
         LA    R1,VARSL
         XR    R15,R15
         MVCL  RØ,R14              CLEAR VARIABLE AREA
         ST    R2,8(,R13)          CHAIN SAVE AREAS
         ST    R13,4(,R2)
         LR    R13,R2              ADDR OF OWN SAVE AREA = ADDR OF VARS
         USING VARS,R13
                                                                EJECT
*********************************************************************
* GET FUNCTION CODE FROM INPUT PARAMETER
*********************************************************************
         L     R1,CPPLCBUF         ADDRESS OF COMMAND BUFFER
         LH    R9,Ø(,R1)           LENGTH OF COMMAND BUFFER
         LH    R8,2(,R1)           OFFSET TO COMMAND PARAMETER
         LA    R8,4(,R8)           OFFSET INCLUDING LENGTH FIELDS
         SLR   R9,R8               LENGTH OF PARAMETER OF COMMAND
         ALR   R8,R1               ADDRESS OF PARAMETER STRING
         LA    RØ,256              MAXIMUM LENGTH WE SUPPORT
         CLR   R9,RØ               PARAMETER STRING TOO LONG ?
         BNH   LLOK1                 NO
         LR    R9,RØ
LLOK1    DS    ØH
                                                                SPACE
         LTR   R1,R9               LENGTH OF PARAMETER, GREATER ZERO ?
         BP    LLOK2                 YES
         MVI   VRC,KPARERR         NO FUNCTION CODE PASSED
         B     LRETURN
LLOK2    DS    ØH
         LA    RØ,8                MAXIMUM LENGTH OF FUNCTION CODE
         CLR   R1,RØ
         BNH   LLOK3
         LR    R1,RØ               MAXIMUM LENGTH
LLOK3    DS    ØH
         BCTR  R1,Ø                - 1
         MVI   VTRTAB+C' ',X'FF'
         EX    R1,XTRT1            SEARCH BLANK
         BC    B'1ØØØ',LNOBL       NO BLANK
         SLR   R1,R8               LENGTH OF 1ST PARAM VALUE: FUNCTION
         BCTR  R1,Ø                - 1
LNOBL    DS    ØH
         MVI   VFKT,C' '
         MVC   VFKT+1(7),VFKT      PAD FUNCTION CODE WITH BLANKS
         EX    R1,XMVC1            STORE FUNCTION CODE
         EX    R1,XTR1             LOWER TO UPPER CASE
                                                                EJECT
```

```
*************************************************************************
* BUILD PARAMETER AREA
*************************************************************************
         AIF   ('&SYSPARM' NE 'NOSVC').SVC3Ø
         LOAD  EP=WRTUSVC
         ST    RØ,VUSVC@
.SVC3Ø   ANOP  ,
         LA    RØ,KFKTINT          INTERNAL FUNCTION
         LA    R1,VFKT             FUNCTION CODE
         STM   RØ,R1,VPARINTF
         OI    VPARINTF+4,X'8Ø'
         LA    R1,VPARINTF
         AIF   ('&SYSPARM' NE 'NOSVC').SVC4Ø
         L     R15,VUSVC@
         BALR  R14,R15
         AGO   .SVC41
.SVC4Ø   ANOP  ,
         SVC   &SVCNR              GET ADDR OF ENTRY IN FUNCTION TABLE
.SVC41   ANOP  ,
         STC   R15,VRC             POSSIBLY RETURN CODE
         LA    RØ,4Ø95             ADDR >= 4Ø96 IN ANY CASE, LOWER: RC
         CLR   R15,RØ              RETURN CODE INSTEAD OF ADDRESS ?
         BNH   LRETURN               YES, ASSUME FUNCTION UNDEFINED
         LR    R1Ø,R15             ADDRESS OF ENTRY IN FUNCTION TABLE
         USING DPARM,R1Ø
                                                          SPACE
         XR    R1,R1
         IC    R1,DNPARM           PARAMETER COUNT
         SLL   R1,2                MULT BY 4: LENGTH OF PAR ADDRESSES
         LR    RØ,R1               ADD LENGTH
         IC    R1,DNPARM           PARAMETER COUNT
         BCTR  R1,Ø                MINUS 1 BECAUSE FUNCTION IS 1ST PAR
         CLI   DPARMAI,Ø           AN OUTPUT PARAMETER ?
         BE    LAPX                  NO
         BCTR  R1,Ø                MINUS 1 BECAUSE OF OUTPUT PARAMETER
         A     RØ,DPARMAL          PLUS LENGTH OF OUTPUT PARAMETER
LAPX     DS    ØH
         MH    R1,=Y(KEPLMAX)      MULT BY MAX LENGTH OF INPUT PARAM
         ALR   RØ,R1               ADD LENGTH
         ST    RØ,VPARMAL          LENGTH OF PARAMETER AREA
         STORAGE OBTAIN,LENGTH=(Ø),LOC=ANY
         ST    R1,VPARMA@          ADDRESS OF PARAMETER AREA
                                                          SPACE
         XR    R5,R5
         IC    R5,DNPARM           PARAMETER COUNT
         SLL   R5,2                MULT BY 4: LENGTH OF PAR ADDRESSES
         ALR   R5,R1               ADDRESS OF 1ST PARAMETER VALUE
         LR    R3,R5
         LA    R2,4                INCREMENT VALUE: LENGTH OF AN ADDR
```

```
         SLR   R3,R2               ADDRESS OF LAST PARAMETER ADDRESS
         XR    R14,R14
LPALOOP2 DS    ØH
         LA    R14,1(,R14)         PARAMETER NUMBER
         CLM   R14,B'ØØØ1',=AL1(1)  1ST PARAMETER ?
         BNE   LPA2                  NO
         LA    RØ,VFKT             FUNCTION CODE
         ST    RØ,Ø(,R1)
         B     LPANEXT
LPA2     DS    ØH
         CLM   R14,B'ØØØ1',DPARMAI OUTPUT PARAMETER ?
         BNE   LPABLANK              NO
         ST    R5,Ø(,R1)           STORE ADDRESS OF PARAMETER VALUE
         A     R5,DPARMAL          ADDRESS OF NEXT PARAMETER VALUE
         B     LPANEXT             DON'T BLANK OUTPUT PARAMETER
LPABLANK DS    ØH
         ST    R5,Ø(,R1)           STORE ADDRESS OF PARAMETER VALUE
         MVI   Ø(R5),C' '
         MVC   1(KEPLMAX-1,R5),Ø(R5)  BLANK PARAMETER VALUE
         LA    R5,KEPLMAX(,R5)     ADDRESS OF NEXT PARAMETER VALUE
LPANEXT  DS    ØH
         BXLE  R1,R2,LPALOOP2
         OI    Ø(R3),X'8Ø'         BIT INDICATING LAST PARAMETER
                                                              EJECT
*********************************************************************
* PARSE PARAMETER
*********************************************************************
         CLI   DNPARM,1            PARAMETER ONLY FUNCTION CODE ?
         BNH   LZXX                  YES
         MVI   VNPARM,1            PARAMETER NUMBER
         XR    R5,R5
         IC    R5,DNPARM           PARAMETER COUNT
         SLL   R5,2                MULT BY 4: LENGTH OF PAR ADDRESSES
         AL    R5,VPARMA@          ADDRESS OF 1ST STORED PARAM VALUE
         LR    R1,R9               LENGTH OF PARAMETER
         BCTR  R1,Ø                - 1
         XC    VTRTAB,VTRTAB
         MVI   VTRTAB+C' ',X'FF'
         EX    R1,XTRT1            SEARCH BLANK
         BC    B'1Ø1Ø',LZX         NO BLANK OR BLANK IS LAST CHARACTER
         LA    R6,1(,R1)           ADDRESS BEHIND BLANK BEHIND 1ST PAR
         LA    R7,Ø(R9,R8)
         SLR   R7,R6               REAMAINING PARAMETER LENGTH
                                                          SPACE
LZLOOP   DS    ØH
         IC    R14,VNPARM
         LA    R14,1(,R14)         NUMBER OF NEXT PARAMETER
         STC   R14,VNPARM
         CLM   R14,B'ØØØ1',DNPARM  LAST PARAMETER ALREADY PROCESSED ?
```

```
         BH    LZX                   YES
         CLM   R14,B'ØØØ1',DPARMAI NUMBER OF THE OUTPUT PARAMETER ?
         BNE   LZ1                   NO
         A     R5,DPARMAL           ADDRESS OF NEXT STORED PARAM VALUE
         B     LZLOOP
LZØ      DS    ØH
         LA    R5,KEPLMAX(,R5)      ADDRESS OF NEXT STORED PARAM VALUE
         B     LZLOOP
LZ1      DS    ØH
                                                          SPACE
         LR    R1,R7                REMAINING PARAMETER LENGTH
         BCTR  R1,Ø                 - 1
         MVI   VTRTAB,X'FF'
         MVC   VTRTAB+1(255),VTRTAB
         MVI   VTRTAB+C' ',X'ØØ'
         EX    R1,XTRT2             SEARCH CHARACTER OTHER THAN BLANK
         BC    B'1ØØØ',LZX          ONLY BLANKS YET
         LR    R6,R1                ADDRESS OF PARAMETER
         LA    R7,Ø(R9,R8)
         SLR   R7,R6                REMAINING PARAMETER LENGTH
                                                          SPACE
         LR    R1,R7                REMAINING PARAMETER LENGTH
         BCTR  R1,Ø                 - 1
         XC    VTRTAB,VTRTAB
         MVI   VTRTAB+C' ',X'FF'
         EX    R1,XTRT2             SEARCH BLANK
         IPM   R15                  SAVE CONDITION CODE, R15=B'ØØCC....'
         BC    B'Ø11Ø',LZ3          BLANK FOUND
         LA    R1,Ø(R9,R8)          ADDRESS BEHIND PARAMETER
LZ3      DS    ØH
         LR    R2,R1
         SLR   R2,R6                LENGTH OF PARAMETER
         LA    RØ,KEPLMAX
         CLR   R2,RØ                LONGER THAN ALLOWED MAXIMUM ?
         BNH   LZ4                   NO
         LR    R2,RØ
LZ4      DS    ØH
         BCTR  R2,Ø                 - 1
         EX    R2,XMVC3             STORE PARAMETER
         EX    R2,XTR3              LOWER TO UPPER CASE
         SPM   R15                  SET SAVED CONDITION CODE
         BC    B'1Ø1Ø',LZX          NO BLANK OR BLANK IS LAST CHARACTER
         LA    R6,1(,R1)            ADDRESS BEHIND BLANK BEHIND PARAM
         LA    R7,Ø(R9,R8)
         SLR   R7,R6                REMAINING PARAMETER LENGTH
         B     LZØ
                                                          SPACE
LZX      DS    ØH
         IC    R14,VNPARM           COUNT OF PASSED PARAMETERS
```

```
         CLI   DPARMAI,Ø           AN OUTPUT PARAMETER ?
         BE    LZX1                  NO
         LA    R14,1(,R14)         TAKE OUTPUT PARAMETER INTO ACCOUNT
LZX1     DS    ØH
         CLM   R14,B'ØØØ1',DNPARM  TOO FEW PARAMETERS PASSED ?
         BNL   LZXX                  NO
         MVI   VRC,KPARERR         PARAMETER ERROR
         B     LFREE
LZXX     DS    ØH
                                                                EJECT
*********************************************************************
* ISSUE USER SVC, PUT OUTPUT PARAMETER TO SCREEN
*********************************************************************
         L     R1,VPARMA@          ADDRESS OF PARAMETER ADDRESSES
         AIF   ('&SYSPARM' NE 'NOSVC').SVC5Ø
         USING PSA,Ø
         L     R3,FLCCVT           ADDRESS OF CVT
         L     R4,PSATOLD          ADDRESS OF TCB
         XR    R5,R5               ADDRESS OF SVRB WE HAVEN'T GOT
         L     R7,PSAAOLD          ADDRESS OF ASCB
         DROP  Ø
         L     R15,VUSVC@
         BALR  R14,R15
         AGO   .SVC51
.SVC5Ø   ANOP  ,
         SVC   &SVCNR              USER SVC
.SVC51   ANOP  ,
         STC   R15,VRC             RETURN CODE
         CLI   VRC,KFKTERR         FUNCTION OK ?
         BNL   LFREE                 NO
         CLI   DPARMAI,Ø           OUTPUT PARAMETER EXISTING ?
         BE    LFREE                 NO
                                                                SPACE
         LA    RØ,1                ONE MESSAGE SEGMENT
         LA    R1,VPLMSGT-4        ADDRESS OF MESSAGE LENGTH PREFIX
         XR    R2,R2
         IC    R2,DPARMA1L
         LA    R2,4+1(,R2)         LENGTH OF MESSAGE INCLUDING LENGTH
         SLL   R2,16                 PREFIX AND LEADING BLANK
         STM   RØ,R2,VPLMSG        INITIALIZE FIELDS OF MESSAGE TEXT
         MVI   VPLMSGT,C' '        BLANK IN FRONT OF MSG, NO MSG PREFIX
         LA    R2,VPLMSG           ADDRESS OF MESSAGE
         L     R3,CPPLUPT          ADDRESS OF UPT
         L     R4,CPPLECT          ADDRESS OF ECT
         MVC   VPUTL,KPUTL         PUTLIST PARAMETER
                                                                SPACE
         XR    R1,R1
         IC    R1,DPARMAI          NUMBER OF THE OUTPUT PARAMETER
         BCTR  R1,Ø                - 1
```

```
         SLL   R1,2                MULTIPLIED BY 4
         L     R5,VPARMA@          ADDRESS OF PARAMETER ADDRESSES
         L     R5,Ø(R1,R5)         ADDRESS OF OUTPUT PARAMETER
         LA    R5,Ø(,R5)           LEFTMOST BIT ZERO
         XR    R6,R6
         IC    R6,DPARMA1L         INCR: LENGTH OF OUTPUT PARAM VALUE
         LR    R7,R5
         A     R7,DPARMAL
         SLR   R7,R6               ADDRESS OF LAST VALUE IN OUTPUT PAR
LPUTLOOP DS    ØH
                                                          SPACE
         CLI   VRC,KFKTUNV         OUTPUT DATA INCOMPLETE ?
         BE    LPUTL                 YES, OUTPUT PARAM FILLED ANYWAY
         LR    RØ,R5
         LR    R1,R6               LENGTH OF OUTPUT PARAMETER VALUE
         IC    R15,DPARMAC         OUTPUT PARAMETER NOW INITIALIZED
         SLL   R15,24
         CLCL  RØ,R14              BEHIND LAST OUTPUT VALUE ?
         BE    LFREE                 YES
LPUTL    DS    ØH
         BCTR  R6,Ø                - 1
         EX    R6,XMVC2            OUTPUT VALUE INTO MESSAGE
         LA    R6,1(,R6)           + 1
         PUTLINE PARM=VPUTL,UPT=(R3),ECT=(R4),ECB=VECB,OUTPUT=((R2)),  +
               MF=(E,VIOPL)          OUTPUT MSG IN ACCORDANCE WITH TSO
         LTR   R15,R15             OUTPUT TO SCREEN OK ?
         BZ    LPUTOK                YES
         MVI   VRC,KPUTERR         RC: OUTPUT FAILED
         B     LFREE
                                                          SPACE
LPUTOK   DS    ØH
         BXLE  R5,R6,LPUTLOOP
LFREE    DS    ØH
         L     RØ,VPARMAL          LENGTH OF PARAMETER AREA
         L     R1,VPARMA@          ADDRESS OF PARAMETER AREA
         STORAGE RELEASE,LENGTH=(Ø),ADDR=(1)
                                                          EJECT
*********************************************************************
* FINISH
*********************************************************************
LRETURN  DS    ØH
         XR    R2,R2
         IC    R2,VRC              RETURN CODE
         LR    R1,R13              ADDRESS OF VARIABLE AREA
         L     R13,4(,R13)         R13 AGAIN ADDR OF CALLER'S SAVE AREA
         LA    RØ,VARSL            LENGTH OF VARIABLE AREA
         STORAGE RELEASE,LENGTH=(Ø),ADDR=(1)
         LR    R15,R2              RETURN CODE
         RETURN (14,12),,RC=(15)
                                                          EJECT
```

```
*********************************************************************
* CONSTANTS
*********************************************************************
XTRT1    TRT   Ø(1,R8),VTRTAB      SEARCH BLANK
XTRT2    TRT   Ø(1,R6),VTRTAB      SEARCH BLANK
XMVC1    MVC   VFKT(1),Ø(R8)       STORE FUNCTION CODE
XTR1     TR    VFKT(1),KUPCTAB     LOWER TO UPPER CASE
XMVC2    MVC   VPLMSGT+1(1),Ø(R5)  OUTPUT VALUE INTO MESSAGE
XMVC3    MVC   Ø(1,R5),Ø(R6)       STORE PARAMETER
XTR3     TR    Ø(1,R5),KUPCTAB     LOWER TO UPPER CASE
                                                          SPACE
KFKTUNV  EQU   4                   RC: DATA INCOMPLETE
KFKTERR  EQU   8                   RC: FUNCTION FAILED
KPARERR  EQU   16                  RC: ERRONEOUS PARAMETER
KPUTERR  EQU   2Ø                  RC: OUTPUT TO SCREEN FAILED
KEPLMAX  EQU   64                  MAXIMUM LENGTH OF AN INPUT PARAMETER
KFKTINT  DS    ØXL8                IDENT FOR INTERNAL FUNCTION
         DC    7X'FF',X'ØØ'
KPUTL    PUTLINE MF=L              PUTLINE PARAMETER PROTOTYPE
KPUTLL   EQU   *-KPUTL
                                                          SPACE
KUPCTAB  DS    ØCL256              TRANSLATION TAB LOWER TO UPPER CASE
         DC    256AL1(*-KUPCTAB)
         ORG   KUPCTAB+C'A'-X'4Ø'
         DC    C'ABCDEFGHI'
         ORG   KUPCTAB+C'J'-X'4Ø'
         DC    C'JKLMNOPQR'
         ORG   KUPCTAB+C'S'-X'4Ø'
         DC    C'STUVWXYZ'
         ORG   ,
                                                          SPACE
         LTORG ,
         DROP  R13,R12,R11,R1Ø     PERMANENT REGISTERS
                                                          EJECT
*********************************************************************
* VARIABLES
*********************************************************************
* NOTE: BECAUSE R13 IS ALSO BASE REGISTER OF VARIABLE AREA,
*       SAVE AREA HAS TO BE LOCATED AT START OF VARIABLE AREA
VARS     DSECT ,                   VARIABLE AREA
         DS    18F                 OWN SAVE AREA
VPARINTF DS    2A                  PAR ADDR FOR INTERNAL FUNC OF SVC
VPARMA@  DS    A                   ADDRESS OF PARAMETER AREA
VPARMAL  DS    F                   LENGTH OF PARAMETER AREA
VIOPL    DS    4F                  INPUT/OUTPUT PARAM LIST FOR PUTLINE
VECB     DS    F                   ECB FOR PUTLINE
         DS    ØF
VPUTL    DS    XL(KPUTLL)          PUTLINE PARAMETER
VRC      DS    X                   RETURN CODE
```

```
VNPARM   DS    X                   COUNT OF PASSED PARAMETERS
VFKT     DS    CL8                 FUNCTION CODE
VTRTAB   DS    XL256               TABLE TO SEARCH CHARACTERS
                                                          SPACE
VPLMSG   DS    ØF                  PUTLINE MESSAGE
         DC    A(1)                ONE MESSAGE SEGMENT
         DC    A(*+4)              ADDRESS OF MESSAGE LENGTH PREFIX
         DC    Y(4+L'VPLMSGT)      LENGTH OF MSG INCLUDING LNG PREFIX
         DC    Y(Ø)                ZERO
VPLMSGT  DS    CL256               MESSAGE TEXT INCLUDING LEADING BLANK
                                                          SPACE
         AIF   ('&SYSPARM' NE 'NOSVC').SVC8Ø
VUSVC@   DS    A
.SVC8Ø   ANOP  ,
         DS    ØD
VARSL    EQU   *-VARS              LENGTH OF VARIABLE AREA
                                                          EJECT
*********************************************************************
* DSECTS
*********************************************************************
DPARM    DSECT ,                   INFO ABOUT PARAMETER FROM FUNC TABLE
DNPARM   DS    AL1                 PARAMETER COUNT OF FUNCTION
DPARMAI  DS    AL1                 POSITION OF OUTPUT PAR (Ø = NONE)
DPARMAC  DS    C                   CHARACTER TO INITIALIZE OUTPUT PAR
DPARMA1L DS    AL1                 LENGTH OF ONE OUTPUT PARAMETER VALUE
DPARMAL  DS    F                   TOTAL LENGTH OF OUTPUT PARAMETER
                                                          SPACE 3
         PRINT NOGEN
         IHAPSA LIST=NO            PSA, POINTING TO TCB
                                                          SPACE 3
         IKJTCB ,                  TCB, POINTING TO JSCB
                                                          SPACE 3
         IEZJSCB ,                 JSCB, POINTING TO PSCB
                                                          SPACE 3
         IKJCPPL ,                 CPPL, POINTING TO PSCB AND OTHERS
                                                          SPACE
         END   AUTHFNC
         AIF   ('&SYSPARM' NE 'NOSVC').SVC9Ø
         PUNCH '   SETCODE AC(1)'  IF CALL INSTEAD OF SVC THEN APF
.SVC9Ø   ANOP  ,
         END   ,
```

Walter Wiedemann
Consultant (Germany)

Remote security

Ask users today and, if they need remote access from home, they want it via high-speed Internet using xDSL or cable modem. And most large organizations have begun to offer it. First the IT security staff, and then senior executives, have been won over by the solid protection provided by RACF, VPN, and a hand-held authenticator such as SecurID.

ANOTHER RISK?

But a new Web site recently highlighted in *Consumer Reports* magazine indicates that a major security risk may have been overlooked: the remote workstation's Internet connection. This new Web site uncovers holes in this connection that hackers might be able to use to gain control of the remote workstation and then get into your corporate network.

It's important to remember that this Web site is based on speculation, not actual incidents of hacker attacks. In the same vein, this article focuses on the potential effect of this speculation on the RACF-protected mainframe environment. All speculation, maybe – but a healthy dose of speculation can also be a proactive way of preventing problems.

A HISTORY

When I first started telecommuting to my local telco in mid-1985, IBM mainframe remote access meant:

- A pair of 9.6Kbps full duplex modems
- A four-wire dedicated line (two-wire was too noisy at that speed)
- 3274 controller
- Coaxial cable
- 3180 terminal.

Within two years, 2.4Kbps dial-up access was being offered to a PC.

It required the use of an electronic security key that you held up to the screen; this read a flickering pattern and gave you an alphanumeric string to type on the emulated mainframe keyboard.

Not much changed over the next decade, though speed increased and SimPC replaced simple VT100 terminal emulation. But then PROFS gave way to Outlook and other Windows NT 4-based workstation services. Now, everyone wanted remote access to the corporate LAN and intranet, not just IBM mainframe and minicomputer hosts.

First, it was ReachOut. This was an interesting concept. You felt like you were controlling a remote workstation that you were viewing on your home workstation – and you really were, as there actually was a dedicated slave PC for each remote user. If you moved the mouse, the mouse cursor moved on a slightly delayed basis on the remote workstation. If you did something that changed very much of the screen, it took a while to refresh fully. Life in slow motion.

The disadvantage was that you couldn't change the options on the minimal set of software on the slave workstation. If it had allowed you to use your office workstation remotely from home, it would have been much better received.

The next approach was to have remote workstations dialling in as remote nodes on the LAN. Now you could use all the software on the LAN that you had on your remote workstation. The only problem was that your LAN connection was running at dial-up speeds. A co-worker trying to test her LAN-based Access 97 application experienced response time as long as half an hour. I think we figured out that 6MB was being transferred across the 28.8Kbps dial-up line. Moments on a LAN were hours on dial-up.

Today, we're back to the remote control model, only this time with Microsoft's Terminal Server. Although dial-up is also supported, high-speed Internet delivers the real performance and is the choice of any remote users doing more than occasional work at home. Both use RSA's SecurID authenticator. Because of senior management's security concerns, high-speed Internet access was a long time coming, and included a lengthy pilot, with Shiva's VPN client added for extra protection.

DEFINING THE RISK

Corporate networks that require VPN and an authenticator from remote Internet-based workstations should be impossible to access *directly* by anyone else on the Internet. But the Web site referred to above demonstrates that each remote workstation's Internet connection must be individually secured. Otherwise, there may be openings for hackers to access your corporate network through one of those remote workstations.

Imagine the following scenario. One of your organization's mainframe technical support staff is spending the summer at home. The children are old enough to amuse themselves, but they do need someone at home, especially to feed them lunch. Every day, at exactly noon, the systems programmer leaves his workstation for a full hour, but leaves it connected to the corporate network and logged on to the mainframe. It takes half an hour before the mainframe session times out and he's disabled that annoying screen saver that locks the workstation after five minutes. After all, his home is a secure environment and he can trust the children.

But what if a hacker were able to monitor that remote workstation, note your programmer's work pattern, and then gain access to the workstation during the first half of the lunch hour? Given the kind of wide-open RACF access many technical support people have, it doesn't take much imagination to see that the hacker could do a lot of damage and have access to a lot of sensitive data.

DEMONSTRATING THE RISK

Gibson Research Corporation's Shields UP! site lets you see for yourself. From http://grc.com either wait 15 seconds or click on the Shields UP! logo. On the Web page displayed, scroll down and click on the Shields UP! logo or CLICK HERE! link.

Although it makes sense to test it on an ISP, either dial-up or high-speed dedicated access, you may be in for some surprises even behind your corporate firewall. These surprises usually begin right on this page. It normally begins 'Greetings', followed by your workstation user ID. If you see your workstation ID, it's visible to anyone on the Internet, including hackers.

Next, push the Test My Shields! button, and watch the long Web page being generated as tests are done on your Internet connection and workstation. But, wait, there's more. Push the Probe My Ports! button on either of these pages. Only ten of the user's 65,535 TCP/IP ports are currently tested, and it takes a little longer than the Shields test. But a freeware high-speed port scanner is under development that will test all of them very quickly.

When I tried it, it seemed pretty clear that 'it could happen to me' just as described above (without the children). Specifically, it was possible to anonymously and remotely connect to my Windows 2000 workstation, but no resources were exposed for sharing on the Internet. Who knows whether I'll be so fortunate when I build a local LAN between my workstation and a test workstation I'm building to run Windows 2000 Server. Even now, I'm still vulnerable to attack by hackers with knowledge of security holes within Windows 2000.

SOLVING THE PROBLEM

So whose fault is this? In theory, these security holes could be plugged for any given remote workstation by:

- The ISP through its firewall.
- The network software, typically part of the operating system, if the Internet connection was automatically configured.
- The ISP through the instructions it supplies to configure the Internet connection for the workstation's operating system.
- The person who installed the Internet connection on the remote workstation, which could be the user or an installer from the ISP or corporate IT.
- The VPN software.

In my case, I recently installed Windows 2000 on new hardware, and then carefully followed my ISP's Win 2000-specific high-speed Internet connection procedures. I haven't yet installed VPN software.

Without doing the same tests with VPN software installed, I'm only guessing when I say that no VPN software addresses this issue. Any

organization that takes this risk seriously would have to test and perhaps fix each remote workstation separately or come up with a global solution that can be run on each workstation. But global solutions are difficult given that most remote workstations are employee-owned home machines completely outside any hardware and software standards that may exist within the organization.

JUST A THEORY?

If hackers hadn't already thought of these forms of attack, they certainly will now that they know about this site – doubtless they read *Consumer Reports* just like the rest of us. And in any case, it seems likely that there were a few hackers among the nearly five million tests that have so far been done using this site.

A final thought: with no known attacks, is talking about this possibility scaremongering, or, worse still, actually encouraging someone to figure out how to do it by giving them the idea? No, not unless you believe that not talking about something will make it go away – and it's hard to imagine any IT security professional surviving very long with that attitude.

Jon E Pearkins
(Canada)

Leaving? You don't have to give up *RACF Update*

You don't have to lose your subscription when you move to another location – let us know your new address, and the name of your successor at your current address, and we will send *RACF Update* to both of you, for the duration of your subscription. There is no charge for the additional copies.

The fuss about passwords and password crackers

For centuries, passwords have proved an easy way to authenticate users, although the protection depends on the user's memory and, of course, on his discretion and security awareness.

Note that in this article, 'cracker' means a cracking tool, not the individual who tries to penetrate a computer system without authorization. A password cracker is a tool that can guess RACF passwords, usually after some tests, based on the information that is managed and stored by RACF. These guesses are not conducted using RACINIT or log-on simulation because the userids would soon become revoked; instead, crackers take advantage of the fact that the method used to encode and store passwords is well known, and can be replayed without using standard RACF procedures.

JUSTIFICATION

It's often said that disclosing exposures improves security and that security through obscurity is a deception. Crackers are designed to help detect the weaknesses of chosen passwords. For example, they allow you to check whether the default password is the same as the default group, or the userid, or a definite string, and so on.

Easily guessable passwords create an exposure, which is all the more sensitive when userids associated with started tasks are involved: it's not unusual for these types of userid to have powerful authorities (operations or even special) and to have a weak password (usually, the password value began as the default group and has remained the same ever since because RACF does not require it to be changed). Weak passwords associated with 'real' humans also create an exposure: anybody can masquerade as somebody else or benefit from a more powerful userid.

The password cracker can be an effective tool for monitoring internal compliance to password standards. It should ideally be used during

security reviews or penetration testing. However, there's no point in using one as part of procedure – much better to cure the evil at the root.

Some security managers use password crackers to convince their management of the need for a tighter level of security. System security is increasingly the responsibility of a part-time administrator, who may not be aware of the vulnerability of the system.

Recent references to password crackers include the following:

- In the World Wide Web Security FAQ, at

  http://www.w3.org/Security/faq/

  "make sure that people with log-in privileges choose good passwords; the Crack program will help you detect poorly-chosen passwords." I think it was referring here to a Unix password cracker – crackers are common in the Unix environment.

- On a military site, at

  http://www.af.mil/news/Feb2000/n20000216_000233.html

  they want "administrators to have the availability of password-cracking tools to identify the use of weak passwords".

- Some RACF user groups also say that "every shop should run some sort of password cracker program at least annually, and before your auditors do". (See *RACF Users' News* # 52, March 2000 Newsletter, on Stu Henderson's Web site at http://home.us.net/~stu/rugnew52.html)

ARE PASSWORD CRACKERS DANGEROUS?

In itself, a cracker poses no threat – if your site is correctly protected, a would-be pirate should not be able to get any information from the bare cracker, even if he arranged to get and install it in his own standard (not APF authorized) libraries.

In fact, however, crackers do require that you pay special attention to strengthening the control surrounding the RACF database (if the tool reads it) or badly-protected copies of the database, or APF libraries (if it gets data through an authorized program).

If weak passwords really bother you, note that a study made by Consul Risk Management (and published in a white paper – 'How much is your mainframe software leaking; statistics on 350 penetration tests') concluded that "the current state of technical security in the world's computer systems is appallingly bad". It discovered that major security 'leaks' were mostly caused by:

- Improper security implementations (in RACF or an equivalent product).
- Program design flaws.
- Programming errors.

It's not unusual to find commercial products that install themselves in such a way (SVC, subsystems, exits, etc) that a knowledgeable insider, with no special authorization, could gain access to all the data and do whatever he wants. It's not easy to write system code that's free of errors and security flaws.

Trivial (or too short) passwords may be the weakest link; however, experience clearly shows that leaky SVCs, unprotected APF-authorized libraries, and unprotected AC(1) programs are generally the problem, and give the pirate quick and easy access. In fact, a weak password may be the first step towards penetration by a hacker; you should consider this type of occurrence as possible and even probable, and do everything you can to limit the damage. A pirate who successfully uses an ordinary account (not a special or operations userid) to penetrate the system should not be able to do much harm afterwards. Remember also that most security incidents are perpetrated by employees, not hackers, and that an insider with the right skill, helped by a security flaw, may ruin your company.

Ironically, it's very easy to persuade somebody that a password cracker is a threat (which it isn't), but much harder to explain that an unprotected system library is a real threat (which it is).

TYPES OF PASSWORD CRACKER

Generally, crackers are non-deterministic: they just try to guess passwords. If they're deterministic, they can guess all passwords –

which is possible if the site still exclusively uses a weak encryption method, such as hashed passwords. (Note that the term ‘hashed’ as used here by IBM is improper; it should be ‘masked’ passwords).

The cracker may work either on-line, in which case it must be run on the current system, with the active RACF database, or off-line, in which case it is run against the security database in some form (a copy, a download by IRRDBU00, or simply a list of all couples (userid, encrypted password) extracted from the database).

The cracker may conduct exhaustive attacks, in which case it successively tries all one-character passwords, then all two-character passwords, and so on. It may succeed if passwords are allowed to be short. Although it’s recently been shown that the DES algorithm is not secure against exhaustive attacks, cracking long passwords (those of seven or eight characters) should take some time on a normal CPU (as opposed to a specialized processor).

A cleverer type of attack is the dictionary attack, in which you try only passwords that make sense for a human, for example you will test ‘POTATO’ but not ‘WZ1H0D89’. The tool I’ve developed (see below) implements this type of attack.

EXISTING CRACKERS

Some security add-ons sold by security software companies (including Consul and RA/2) contain embedded RACF password crackers. Others were offered by individuals, including Nigel Pentland’s CRACF to be run on a PC (see http://www.cairnleck.co.uk/nigel/).

My interest in password cracking began in the 1980s when I discovered by accident that I could crack every password in the shop where I worked, which used not DES but the weaker ‘hashed’ encryption. Although I was only a novice in cryptography, IBM provided the required interface (RACXTRT TYPE=ENCRYPT), so it was easy to write an Assembler program that would guess passwords. By trying all characters successively, it could decrypt the first byte of the password, then the second, and so on. This was a deterministic cracker, in the sense that all (not DES-encrypted) passwords could be

recovered. This doesn't work for DES, because DES is a block cipher: that is, it works on a 64-bit basis, not byte by byte.

DESCRIPTION OF A DICTIONARY ATTACK CRACKER

Since then, I've been developing a more powerful password cracking program, using a dictionary consisting of many English, French, and Spanish words. The program can generally decrypt between 2% and 50% of all passwords. The passwords have to be provided either in encrypted form, or extracted from the active RACF database (in which case APF authorization is required as it does a RACXTRT TYPE=EXTRACT call). When the encrypted password is known, it encrypts clear-text passwords from the dictionary and checks whether the result matches the encrypted password – if it does, the password is cracked. Some parts of the source have been unveiled on my site. Here is some pseudo-code that gives an idea of the processing:

```
loop 1: read userid in //SYSUSER
if encrypted password for this userid not supplied, become APF and go
get it (asking RACF)
loop 2: read 8-byte clear-text password in //SYSIN
transform it into an encryption key
use it to encrypt the userid
if the result matches the encrypted password, password for this userid
is « cracked »
loop
loop
```

Note that the term 'encrypted password' is improper, because the password is not encrypted; rather, it's used as an encryption key to encrypt a fixed string, the userid. This is a one-way encryption that cannot easily be reversed (and never need be, in current functioning). Nowadays, we would use a message digest (or fingerprint) of the password, which is a more modern type of one-way function. Although this isn't secure against dictionary attacks either, the big plus is that the password length may be arbitrarily high (PGP uses the same concept with its 'passphrases').

PRECAUTIONS AROUND PASSWORDS

Unfortunately, password validation is not a standard part of RACF.

The only way to ensure that passwords are not weak is to enhance the validation rules used at the time they are chosen by the end user. So you have to check the length of passwords that you permit and the password rules.

Some kind of password tutorial should be used to teach users not to pick weak passwords. They need to understand that selecting a strong password is the single most important thing they can do to protect their information from unauthorized access. Once a single user account is compromised, an expert cracker (the individual, not the tool) can exploit security holes in the system (as described above) and break into special accounts or gain access to all data.

But it's important not to be too aggressive. I heard of one site that insisted on consonant-only passwords. Though this may be acceptable in some countries, it makes you wonder how people can be expected to remember their password.

The new password exit ICHPWX01 is the only way to carefully filter weak passwords. But you also need to check the password expiry rules and make sure that passwords are changed regularly. Accounts should be disabled after a predefined number of failed attempts to authenticate (in general, the limit varies between three and ten attempts).

I think RACF's major weakness lies in having a maximum length of just eight characters for the password. Passphrases would be a good alternative, but IBM is unlikely to offer them as the password input zone on screens would need to be enlarged. This is a pity, because long sentences may sometimes be easier to remember, and would be harder to crack than short passwords.

The RACF Password Encryption exit (ICHDEX01) could be used to get rid of the DES algorithm and install another less well-known algorithm, for example a MD5 or SHA variation, or Blowfish, which resists dictionary attacks rather better. But this is clearly not a definitive answer to the problem of weak passwords. By the way, make sure that you check on your site whether the default ICHDEX01 has been uninstalled in the LPALIB; this disables the usage of the DES algorithm in favour of hashed passwords. Note that some one-time password products (like SecurId) modify ICHDEX01.

Recent versions of RACF enable you to dispose of weak passwords associated with started tasks rather than real humans, by using protected userids with no password and no possibility of logging on or submitting batch jobs.

Needless to say, the RACF database should be UACC(NONE) and its access list should be very short. It's very easy to extract encrypted passwords from the database (a REXX exec can do it) once you have read access. Remember that anyone who has READ access could potentially use any existing password cracker.

DOING WITHOUT PASSWORDS

IBM has long recognized the inherent weakness of passwords, and recent years have brought new means of authentication. For instance, we now have PassTickets – cryptographically-generated, single-use, short-lifespan password substitutes. These are described in my article 'Authentication using the RACF PassTicket' (see *RACF Update* May 2000). The weak link with PassTickets is the secret session keys that must be securely stored. More and more single sign-on products support RACF PassTickets, the secret keys being stored on a supposedly secure server. An alternative is not to use secret keys but simply to generate the PassTicket on MVS and pass it to the client via a secure channel (as, for example, in Neon Systems' Halo/SSO).

Challenge-response devices, or one-time non-reusable passwords generated by tokens like the RSA SecurID from Security Dynamics, mean that the user no longer manages the password and it simply cannot be guessed. These also resist network sniffing.

Other, not widely-used, solutions include smart cards, often used to lock workstations, and biometrics, which uses some physical characteristic that uniquely identifies you (fingerprint, iris, voiceprint, signature written on a pressure-sensitive pad, etc). But security measures such as these really seem over-intrusive, and don't make security easier for the end user.

DCE Security server or the LDAP server are technologies geared to distributed applications; this positions RACF as a central point for

remote authentication. LDAP on OS/390 may provide an open limited interface to RACF, and many single sign-on products will use it in the future.

Powerful cryptographic methods are also enabling breakthroughs. Recently introduced to OS/390, Kerberos allows authentication across unsecured networks. It was developed at the MIT, and named for the three-headed watchdog from Greek mythology, who guarded the entrance to the underworld. Kerberos is now offered with OS/390 Version 2 Release 10. This means that a Windows 2000 client user can be authenticated by RACF. Kerberos is in fact another single sign-on system, using a mutual authentication model, which never sends users' passwords across the network. However, Kerberos is not a cutting-edge product, because it implements complex protocols based on conventional (symmetric) encryption algorithms.

SSL (Secure Sockets Layer), first introduced to OS/390 in Version 2 Release 6, is a communication protocol based on the concept of public-private key pair cryptography and digital certificates. Keys are unique to each server (and optionally to each client, with SSL Version 3). The server provides a digital certificate to ensure its identity. Data is encrypted using public keys; only the private key can be used to decrypt data. The beauty of all this is that no secret information needs to be disclosed or shared between parties (unlike PassTickets, Kerberos, or the standard RACF password). SSL has a strong Web connotation, but it can be used with tn3270 to connect to TSO, CICS, etc. Even if neither the client nor the server is authenticated by SSL, at least the flow of data is encrypted and the regular RACF password can be passed without being compromised in the network.

RACF today can permit access based on the contents of a certificate (this is used for Web applications built on WebSphere). In this particular case, the RACF password has become history, although it's conceivable that the certificate is protected by a password at the workstation. I view public key encryption and Public Key Infrastructures (PKI) as the most promising field for reinforced authentication.

MY PASSWORD CRACKER

My password cracker can be downloaded from my site, at

http://os390-mvs.hypermart.net/cracker.htm

You just need to send me an e-mail to decipher the installation file (so that I can control who gets the program). Use with moderation, but determination!

Thierry Falissard
(France)

Call for papers

Why not share your expertise, and earn money at the same time?

RACF Update is looking for REXX EXECs, macros, program code, etc, that experienced RACF users have written to make their lives, or the lives of their users, easier. We also publish longer, analytical pieces, and 'hints and tips' type articles.

Your article will be vetted by our expert panel, and we'll send you a cheque when it's published. Articles can be short or long, and can be sent or e-mailed to Fiona Hewitt at any of the addresses shown on page 2.

Why not call now for a free copy of our *Notes for Contributors*, or look on our Web site, at

www.xephon.com/contnote.html

Web user identification

Nowadays, many large Web sites access a mainframe protected by RACF. At first, only the most innocuous of data was made available through the Web site. But things have gradually changed, not just with e-commerce, but also with access to user-specific information for which privacy must be protected. Security, in the form of user identification, is now a requirement. But how can it be achieved?

INFINITE VARIETY

More and more large Web sites now perform user identification, typically beginning with a one-time registration process. Ignoring the obvious question of "why?", I have instead become intrigued by the wide variety of approaches to authentication.

This morning, I went from being intrigued to being mystified. I always thought that I had at least a vague notion of what was going on behind the scenes. But my brother-in-law pointed out that a freshly redesigned Oracle Web site knew his and a co-worker's name, despite the fact that:

- He had never identified himself in the past to the site.
- His name was not in his workstation's user identification fields of Microsoft Office or elsewhere.
- He had gone through a corporate proxy server that should hide his identity.

In this article I've chosen not to speculate on how each of the Web sites actually implements user identification. Rather, I've looked at each one from the user perspective. After all, the success of a Web site depends on keeping your visitors happy and coming back often.

SIMPLE, YET RELATIVELY PAINFUL

http://www.absound.com

I have been shopping at A&B Sound for about 30 years. Years ago, I

registered by giving my name, address, phone number, and e-mail address. They assigned me a six-digit customer id number, but I was allowed to choose my own password in the four to eight character range.

Every time I place an order, I must re-key my credit card information. Although I don't find this a problem, as I've been adding to the same order for almost a year (and will probably continue to do so indefinitely), it could obviously be annoying.

Much more frustrating, because of its frequency, is the request for customer id and password that occurs every time you add something to your on-line shopping cart. Internet Explorer's AutoComplete feature is no help here because it relies on remembering URLs to determine when to insert id and password on a Web page you've previously visited. But the URL of this page is different each time you push the *Add to Cart* button because the UPC (bar code on the product you are ordering) is part of the lengthy URL. Admittedly, however, once you've typed your customer id, AutoComplete does enter your password for you.

AutoComplete is even less help when looking up an order. Even though the URL is fixed, AutoComplete doesn't even supply the password this time, let alone insert the customer id.

The problem is that it doesn't recognize the Web page as one containing an id and password. This is clear from the fact that it never prompts you to have it remember them. The only thing odd about the page, and the likely problem, is the sizable distance between the user id and password field titles and the fields themselves.

A good idea, but risky

Whenever you create or add to an order, A&B sends you an e-mail. Among other things, this includes the URL of the Check Order page. This is a great idea, and a great help to the user. But the next decision has traditionally been a tough one: should the e-mail be in text or HTML format? Here is the trade-off:

- Not all e-mail packages will create a link for an URL included in a message; without it, users must select, copy, and paste the URL into a Web browser.

- Some e-mail packages make HTML messages more difficult for users to handle than text-based ones.

A&B made its decision – text – several years ago when it first introduced the site. Today, HTML is almost universally well handled by e-mail packages. And the vast majority of users have e-mail packages that automatically create links for URLs. Maybe it doesn't matter, but my personal best guess says that HTML is currently the right choice.

http://www.outofprintmusic.com

Out of Print Music goes two steps further, filling in the id and password fields for the user. Their text e-mail includes an URL:

http://outofprintmusic.com/shopping_cart/view_status.asp?OrderID=131642013&Password=J6166717

While no one can argue that this is the ultimate in user-friendliness, it raises a lot of red flags in terms of security. Why isn't the Web page SSL-protected (https)? Without SSL, the id and password are being transmitted in the clear, without encryption, from the user's browser to the Web site. Not once, but twice. First, in the URL, during the transmission that requests the page. Then again, in the form, in the transmission that submits the form.

And what of the e-mail itself? It's a widespread practice to send passwords to users via e-mail when they first register, whenever they change their password and, on request, whenever they forget their password. Again, all in the clear, without encryption.

One way to analyse this risk is to understand its source: hackers. Although they might monitor random Internet traffic, the chances are extremely low – given the volume of Internet traffic versus the number of hackers – that a single Internet transmission will be monitored by anyone. Hackers are much more likely to target Web sites with non-trivial traffic flows, especially those doing e-commerce or with sensitive information. It's quite conceivable that both Web and e-mail traffic to and from a popular Web site would be monitored periodically.

http://www.ebay.com

Sites whose only business is their Web site might be expected to spend more time 'getting it right' than others. Perhaps the best known Web-only business is eBay, with, at any given moment, several million items on 1-2 week auction.

To encourage window-shopping, eBay requires user identification only where it is needed, namely: to bid on an item, to sell an item, and to view the e-mail address of a seller or bidder.

Whenever you attempt to perform any of these three actions, you're prompted for your id and password. Although not all of them are shown on the user identification page that's displayed, eBay actually offers you six options:

- If you have no eBay user id, you can register and get both id and password.
- If you forget your password and you defined a password hint during or since registration, you can get your password immediately. Despite its name, the password hint is actually a question and answer unrelated to the password, except for the fact that eBay will display your password only if you answer the question correctly.
- If you haven't established a password hint, you can e-mail eBay with your user id, name, and street address to have instructions e-mailed to you within 24 hours that will allow you to change your password.
- You can enter your id and password each time you want to perform an action requiring user identification.
- You can sign in once and not be re-prompted so long as you don't let the temporary cookie expire by leaving 40 minutes between eBay page views or closing your browser.
- You can sign in with SSL.

The *My eBay* feature gives you even greater control. Under the

Preferences tab, *Sign In Preferences* allows you to specify any areas where you still want to be prompted for your password, even after you sign in. No matter what, you're always prompted for your password when you try to change your credit card or user registration information.

PERPETUAL LOGON

Two of the major eBay wannabes, amazon.com and Yahoo!, were also founded as Internet businesses. Having dabbled in their auctions for out-of-print books, I find that their prices for popular items are often lower because there are fewer bidders than on eBay. So, bigger is not necessarily better – for the consumer anyway.

http://www.amazon.com

There is also the convenience factor. Having registered years ago, I see "Hello," followed by my name every time I hit the Amazon home page. Click on the *Auctions* link and the greeting repeats, but with a parenthetical choice: "(If you're not" then my name, then "click here.)"

I also updated my amazon.com registration when I first started bidding on amazon auctions, adding a user id so that I would blend in with the crowd.

http://www.yahoo.com

Although there's no indication that Yahoo! knows you when you hit its home page, when I click on an *Auctions* link, the grey banner bar near the top of the page says "Welcome," and refers to me by my user id.

THE MOST ANNOYING

http://www.freespeech.org

To date, I've found only one site that assigns you a password and doesn't allow you to change it. One of the best-run free Web hosting sites, freespeech.org, specializes in RealAudio and RealVideo. As the

name implies, its objective is to allow those without the broadcast media's megabudgets to reach an international audience.

Worse yet, it hasn't even learned from CompuServe and others who, at least, assign passwords made up of real words. Believe it or not, freespeech.org gives you eight random lower-case letters and numbers and will not recognize them if any are entered in upper case.

THE WEIRDEST

http://www.globefund.com

Canada's *Globe and Mail* newspaper has been running an investment Web site for nearly five years. One of globefund.com's most useful features is the ability to create a list of mutual funds or stocks that you want to keep track of. Bookmark your favourite report summarizing the performance of the funds in your fund list, and you can check current prices just by clicking on that Favourite.

When I recently migrated from Windows 98 to 2000, changing my workstation user id in the process, I was careful to copy my cookies across from the old workstation to the new. I also changed the user id that forms a part of the file name of each cookie. My cookies worked on every other site I tried except globefund.com.

In the back of my mind, I remembered reading about globefund.com somehow tying you to your workstation. And, sure enough, one of the Help pages mentions that all users of a workstation share the same Fundlist.

When I first started using globefund.com, its fundlist was the first good reason I had to accept a cookie. I remember looking at the cookie, and being surprised that it didn't include my fundlist entries. They are, of course, stored in a database on its Web site.

ANNOYING TREND

One of the most annoying trends is among informational Web sites that are run as businesses unto themselves. Until recently, these relied on banner advertising and similar types of sponsorship to make

money out of freely supplying useful information to Web visitors. But many are now beginning to offer more valuable information, still for free, but at a price in convenience and unsolicited contact. This better information is offered only after the user completes a one-time registration and logs on.

BUCKING THE TREND

While endless numbers of Web sites have followed the trend to add user identification to all or part of their site, Microsoft and IBM are big enough to create trends of their own. Both have expanded, not reduced, the amount of detailed technical information they provide electronically, and the amount they provide without requiring an id and password. I use the word 'electronically' because neither began on the Internet, instead running their own networks. And both offered substantial subsets of their technical information offerings on proprietary networks such as CompuServe.

http://www.ibm.com

IBM began with IBMLink, first released to customers in the early 1980s, and viewed by IBM as a form of customer self-service – a way to cut customer support costs by reducing the number of queries that harried IBM system engineers had to answer.

In the mid-1990s, IBMLink was gradually implemented on IBM's Web site. From the beginning, unlike the proprietary network, the Web site at

http://www.ibmlink.ibm.com

offered some information without the need to log on. The amount of information grew, first for users who logged on, then for everyone. Finally, one day not too long ago, the option to log on disappeared altogether.

Separate from IBMLink, over the last few years, IBM began offering most of its manuals on its Web site. The System/390 library is at

http://www.s390.ibm.com/os390/bkserv

Even relatively technical material, such as the popular Redbooks, is offered on-line at:

http://www.s390.ibm.com/os390/bkserv/redbooks.html

Of course, as their name implies, IBM licensed manuals are still available only to customers who have the relevant hardware or software licensed. These are logic manuals and similar deeply technical material that IBM would prefer its competitors not to get their hands on – it's now been over ten years since IBM stopped offering source code for any new products, versions and releases.

http://support.cai.com

Many of the large software vendors have followed suit, though it took a while. Sterling Software, for example, probably because of the high selling prices for its paper manuals, did not offer even CD-ROM-based manuals when I inquired in early 1997. It does now, of course, and if they don't already have their manuals on-line, its recent acquisition by Computer Associates (CA) will certainly ensure that it does soon.

http://www.microsoft.com

Although Microsoft has been faulted for not seeing that the Internet would quickly displace proprietary dial-up networks like CompuServe, AOL, and its own msn, it was one of the first to offer its support database on-line, without charge. Knowledge Base was even available on competitive proprietary networks, like CompuServe. Today, it's one of the most popular places on Microsoft's Web site.

But the business case was pretty strong. Microsoft needed a way to fight the criticism it received for lousy support. Back in the days when telephone support was free, 30-40 minutes on hold was not unusual. Making the same database that their Help Desk staff used available on-line was a pretty obvious solution.

ANOTHER TREND

Another recent trend is to use the e-mail address as the user id. Having

read 45 years' worth of *Consumer Reports*, my consumer rights concerns are alerted when I see this trend. Here is why.

During registration, many sites position privacy statements near the e-mail address field, not so much to satisfy privacy watchdog organizations, but because they know that people hate what used to be called spam. I say "used to be" because the so-called anti-spam law in the US hasn't managed to stop marketers from buying the complete database of millions of Internet domain name registrants, and e-mailing them all – many even include a statement like "This message cannot be considered spam" and then quote a section of the law.

The point is, that by making the user's e-mail address his id, Web sites (whether they realize it or not) have found a clever way to put most users off their normal guard. Instead of being an information field within the registration form, which could raise spam concerns, it looks more like a helpful way to avoid creating and remembering yet another user id.

TURN-OFF FACTOR

You need to be sure, before you implement user identification on a Web site, that you have really good reason to do so. The one-time registration process and/or the on-going entry of user id and password are bound to irritate many of your visitors, who will leave the site and probably never return.

If user identification becomes a requirement rather than an option, you should ensure that it's used only where needed. Something is very wrong if the first thing a visitor has to do on a corporate home page is register or log in. Visitors should have free (read-only) access to public information such as press releases and product/service descriptions, without the need for user identification.

Sites that also require SSL 128-bit encryption should take an extra-careful look at exactly where it's really required. Although this might not seem important now that there's an exportable version of 128-bit encryption, don't forget users with older browsers. It makes sense to require 128-bit encryption only where it's justified. This is typically a subset of where user identification is required – and many sites don't require it at all.

I'm not advocating a wholesale abandonment of encryption. But there are certainly medium security situations where 40-bit encryption would suffice. SSL could be used, with 128-bit encryption where the user's browser supports it, and 40-bit otherwise.

CATALOGUE SHOPPING

So far, I've focused on one-time registration and log-on as an annoyance. Until very recently, Sears Canada was proof that lack of such a process can also be annoying – every on-line order required you to enter your complete name, address, phone, and other information. Because I'm a touch typist, the trade-off is worth it, and I'm willing to go to the effort of writing down an id and password.

Is there a better alternative – one that's more convenient without unnecessarily compromising security? A permanent cookie would be one solution, but it has two disadvantages. It is both workstation and user id dependent. A cookie resides on the workstation, and is accessed only when a specific workstation user id is logged on.

Second, the workstation environment can't be considered secure. Many Windows users never see a workstation log-on screen. Those that do, log on in the morning and log off at night, often leaving their workstation unattended during the day. Office workstations are rarely shared, but even when protected by workstation locking that detects a given period of inactivity, this is generally set so high (eg 15 minutes), to avoid inconvenience to the user, that it's an easy target for the observant office criminal. Home workstations are rarely shared beyond household members, but that doesn't prevent the children's hacker-minded friends from doing a lot of damage. No consumer will accept responsibility for this kind of unauthorized use.

There's no easy answer, but it's a problem that deserves a lot of thought.

LESSONS FROM RACF SINGLE SIGNON

It might not seem such a big deal to have to remember one id and password. But most Internet users visit a lot of Web sites and, even if you register only when absolutely required and stick as closely as

possible to the same id and password for all sites, you can easily end up with a list of 50 exceptions: ids and passwords for 50 different sites that don't allow your chosen id and password. And that's not counting the sites that use your e-mail address as your user id.

When I mentioned this problem to an only slightly computer-literate friend, she suggested what I had been thinking based on my RACF background. Why not register users once for all participating Web sites, by transparently taking the user to the central registration site. That site could run an authentication server, just as RACF does with Single Sign-on, transparently passing user identification tokens to the Web site the user is currently visiting. This could even provide the basis of a new Internet business....

DECISION POINTS

Below, I've listed a starter set of questions you need to consider when planning your Web user identification. You will undoubtedly find many more.

- Choose your own user id?
- Length of user id?
- Choose your own password?
- Length of password?
- Id and password remembered through a session?
- Id and password remembered between sessions?
- Can id and/or password be remembered by Internet Explorer's Autocomplete function?
- Delivery address remembered in a profile?
- Does the Web registration form allow addresses and phone numbers in all possible world-wide formats?
- If there are any restrictions on users, such as age or geographic location, is this stated at the very beginning of the registration process?

- Are these restrictions checked by putting fields at the very beginning of the form that are automatically checked before allowing the user to proceed to the remainder of the registration process?
- Payment information (eg – credit card type/number/expiry) remembered in a profile?
- E-mail confirmation of order includes link to order status page? In HTML format so the link is live for all e-mail packages? With ID filled in? With password filled in?
- Does AutoComplete recognize the Web page as one containing ID and password?
- How are forgotten passwords resolved?
- Finally, the media coverage of credit-card-number-stealing hackers has made many users aware of the little padlock at the bottom of their browser screen. So, are passwords entered on SSL (https://) protected screens?

George Walker
(Canada)

Code from *RACF Update* articles

As a free service to subscribers and to remove the need to rekey the scripts, code from individual articles of *RACF Update* can be accessed on our Web site, at

http://www.xephon.com/racfupdate.html

You will need the user-id shown on your address label.

Information point – reviews

INTERNET CONNECTION SECURITY

It's been a long time since I last heard of SpinRite, and the Gibson Research site at http://grc.com confirms that Version 1.0 was released in 1988. But it's not the current Version 5.0 that's of interest here. Shields UP! is discussed in detail in the *Remote security* article elsewhere in this issue. There, you'll see what it reveals about supposedly secure access to RACF-protected mainframes from remote workstations via VPN.

SPYWARE

Also on the site is the OptOut home page, at

http://grc.com/optout.htm

This provides a gateway to a thorough discussion of what Steve Gibson terms 'spyware' – any software that quietly sends information back to its creator, without the user's knowledge, from the user's workstation through the Internet.

Of course, the uses of this kind of information range from the 'good' (such as researching usage patterns to assist design decisions for the next version of the software product), to the 'bad' (selling the statistical information obtained), and the 'ugly' (offering user-specific data to the highest bidder). But these are issues of privacy, not corporate IT security.

However, the same approach could be used for industrial espionage, allowing your competitors, the media, or any group that objects to your business, to obtain sensitive data from your corporation.

Now you're obviously not going to see that kind of behaviour from the large software companies that already use spyware-like techniques. The risk of prosecution and drop in their stock price is too big a price to pay. But economics and national laws are very different elsewhere in the world. Pick a country where:

- Software experts are paid 1/30th what they are in the US, and
- It's culturally acceptable to rob tourists because they're rich foreigners.

The result: a perfect atmosphere for an industrial espionage firm to do its dirty work. Create a useful free software package with hidden spyware capabilities, market it well in North America and Europe, and, before you know it, it's being run in major corporations.

Gibson's OptOut home is really a Web site within a site. There's much too much for one page, but between the page itself and the 11 other pages that are linked to, you'll find:

- His spyware definition.
- His proposed code of conduct.
- Lists of known and suspected spyware.
- OptOut software download and FAQs.
- Links to articles, Web pages, discussion groups, and FAQs on Internet privacy issues.
- A description of the Internet Spyware Analyzer used internally by Gibson Research.

OptOut is currently freeware, but it only detects and removes spyware from Aureate. A more comprehensive product is currently in development, but there will be a charge for it. The Internet Spyware Analyzer is not for sale.

SECURITY MANAGEMENT ASSESSMENTS

BMC Software is currently offering two on-line Security Management Assessments at

http://www.bmc.com/assessment/security

One looks at security administration and the other at audit and e-business capabilities. Each asks a short series of yes/no questions, and then gives you the results on-line. Even though both are part of a marketing campaign for CONTROL-SA, they do include many of the

embarrassing questions you would be asked in a professional security audit.

IBM'S RACF HOME PAGE

A search for 'RACF' on IBM's home page, at

http://www.ibm.com

returns a lot of hits. And, as it should be on all sites' search facilities, the RACF home page is listed first, at

http://www.s390.ibm.com/products/racf/racfhp.html

The home page begins by stating that RACF will be celebrating its 25th anniversary very soon. It then points out that RACF is part of the SecureWay Security Server for OS/390, and that references to SecureWay may apply equally to RACF.

The left sidebar of the RACF home page has a number of links: overview, what's new, year 2000, VM, downloads, user groups, on the road, migrating, library, related links, FAQs, and 'contacting us'. Although some of these options don't look too promising, it's worth persevering. For example, when you click on *Year 2000*, you'll be greeted by a page that begins 'As the year 2000 approaches'; but the page actually contains useful information on RACF date formats and the date windowing issues they create.

On-line manuals

The *Overview* offers a choice of Shockwave and non-Shockwave versions of two articles excerpted from *OS/390 Security Server (RACF) Introduction* intended to provide a technical overview of RACF:

- 'The Benefits of RACF Security'
- 'RACF Record-Keeping'.

Clicking on the *OS/390 Security Server (RACF) Introduction* link gives you access to all RACF on-line manuals. You'll also find a link

to the *OS/390 Security Server (RACF) Information Package CD-ROM* (see below).

From the RACF home page, the *What's New* link offers a brief description of features recently added to RACF. And at the bottom of the page, 'RACF in the Press' offers RACF-related articles written by IBMers in Adobe Acrobat format.

The *VM* link provides a brief summary of the new features in the latest version of RACF for VM. The page begins with a link to the official IBM announcement letter, if you want all the details. You can also download or read on-line the *Program Directory* in Adobe Acrobat format: the same 176 pages of installation instructions you'll receive on paper with the installation tape.

Free utilities

The *Downloads* link provides brief descriptions of six utilities available from the *S/390 FTP Server*. Click on the name of any of the six utilities for a detailed description and downloading instructions, either directly from the Web page through your browser, or with FTP. Click on *S/390 FTP Server* and you have direct FTP access to all of these utilities, each shown as a folder you can double click on to open. Each folder contains the installation materials for one utility. A readme file in Adobe Acrobat (.pdf) format is also available.

Further down the *Downloads* page, the RACTRACE utility is offered for download. Click on it and you're placed in an FTP screen with a readme file and a zipped version of the 113KB utility.

RACF User Groups lists the cities known to have a local RACF User Group (RUG). The three RUGs that have Web pages of their own are listed as links.

On the Road is a periodically updated list of where IBM's RACF experts will be speaking. Like the RUGs list, it lists only North American locations.

Migrating

'Migrating' offers information and links to information on virtually every migration scenario:

- Replacing a non-IBM product with RACF.
- Moving from one version/release to another of RACF or OS/390 Security Server.
- Moving from RACF to OS/390 Security Server.

The page begins with a link to *IBM's Software Migration Project Office – Tivoli Migration Team*. One of their primary goals is to support the displacement of non-IBM security products with RACF, supplying a lot of hands-on help in the process.

Information on each version/release of OS/390 Security Server is provided. Recent releases of RACF are also included for MVS and VM. The *VnRnn* links display the release-specific announcement letter. Where applicable, withdrawal dates are shown. Links to migration manuals are provided for most releases of both OS/390 Security Server and RACF in both BookManager and .pdf (Adobe Acrobat) formats.

The *Library* link gets you to the same page as the *OS/390 Security Server (RACF) Introduction* link mentioned above – a list of all RACF on-line manuals.

Related Links provides a list of useful IBM pages. The only exception is the RACF-L discussion list. Though useful, this is run by the University of Georgia, not IBM. The *Links* page is broken up into the following categories:

- IBM SecureWay Security Server components
- IBM's SecureWay security information
- IBM security on various platforms
- Other IBM security products
- Other links

- Documentation
- Discussion lists.

At the bottom of the page, you'll find a link to the *IBM Technical Support Technical Information* site, containing "a wealth of presentations, white papers, and tools."

FAQs

The FAQs link leads you to a huge collection of questions and answers, divided into four sections:

- RACF Remote Sharing Facility (RRSF)
- RACF and MVS TCP/IP
- RACF in the year 2000
- RACF technical tips.

The majority of questions are in the first section (RRSF), and are further divided into 19 categories:

- Synchronizing passwords
- Sharing a RACF database between MVS and VM
- The RRSF node name
- Shared RACF database
- Directing commands
- Restricting the execution of a command to one system
- Using the ONLYAT keyword
- The workspace datasets
- Setting the CDMF key
- The RRSFLIST dataset
- Terminating RRSF
- Terminating RRSF connections

- Abnormal termination of a connection
- Generic qualifiers in the APPC/LU profile
- Protecting the APPC utility that creates the DBTOKENS
- Changing RRSF definitions
- A target node is down
- Audit records
- The number of tasks handling commands in the RACF address space.

RACF CD-ROM

Details on the OS/390 Security Server (RACF) Information Package CD-ROM at

http://www.s390.ibm.com/products/racf/racfbroh.html

quickly demonstrate that it is a very worthwhile subscription offering. It is usually revised quarterly, and brings all RACF-related information together into one place (multiple CD-ROMs).

Most of its material, currently 650 of its 850 publications, consists of the manuals from other MVS and VM program products that include RACF considerations. The remainder is manuals from multiple version/releases of RACF and OS/390 Security Server, as well as:

- ITSO Redbooks related to RACF system security.
- Flyers.
- Education course listings.
- RACF graphic bitmap.
- Sample code, including the RACFICE tool for creating reports and the DBSYNC exec for comparing and merging two RACF databases.
- Adobe Acrobat (printable) files for Security Server and RACF product manuals.

- Related Installation Materials (RIMs) for RACF.

You can purchase the subscription as a feature of OS/390 or RACF Version 2. The OS/390 feature code is 8004, and 9006 for RACF. The price is a one-time charge of US$275.

Alternatively, you can order the publication, Order Number SK2T-2180, but how much you will be billed is not clear. This Web page states a price of US$100 for a single copy or each copy delivered as part of a subscription. IBMLink's Publications Catalogue lists prices of US$50 and UK£35.14.

REDBOOKS

Redbooks detail the work of IBM's International Technical Support Organization (ITSO), which partners with all IBM Divisions, including Lotus and Tivoli. Today, Redbooks runs a comprehensive Web site at

http://www.redbooks.ibm.com

From the home page, the left sidebar gives you 11 options:

Redbooks online, just published, Redpieces, Redpapers, residencies, CD-ROMs, additional materials, how to order, about Redbooks, 'contact us', and registration.

Redpieces are Redbooks that have yet to be completed. Click on one, and you'll see a Web page with an abstract, a table of contents, the date first posted, the date of the last update, the planned publishing date, the names of the authors, a link to e-mail your feedback, and a view on-line link.

To actually see the Redbook in its current state, click the small *View On-line* link in the upper right-hand corner of the page. Assuming you have Adobe Acrobat Reader installed on your workstation, you'll then be viewing the manual, with portions of the document downloaded as needed, as you view different pages.

For anything more than a brief glance, it probably makes more sense to download the entire manual to your workstation. With Microsoft

Internet Explorer, a right-click, then selecting 'Save Target As' from the pop-up menu, will do the download.

Redpapers will never become Redbooks, even though many are quite lengthy. They're written to address a specific topic, but aren't necessarily the product of an ITSO residency. Not available in hard copy, they're offered on-line in almost the same format as Redpieces, with abstract, table of contents, and link to the Redpaper itself in Adobe Acrobat format.

Jon E Pearkins
(Canada)

Free weekly news by e-mail

Four weekly news services are available free of charge from Xephon, covering the following subject areas:

- Data centre
- Distributed systems
- Networks
- Software

Each week, subscribers receive, by e-mail, a short news bulletin consisting of a list of items; each item has a link to the page on our Web site that contains the corresponding article. Each news bulletin also carries links to the main industry news stories of the week.

To subscribe to one or more of these news services, or review recent articles, point your browser at http://www.xephon.com.

Contributing to *RACF Update*

In addition to *RACF Update*, the Xephon family of *Update* publications now includes *CICS Update*, *MVS Update*, *TCP/SNA Update*, *VSAM Update*, *DB2 Update*, *AIX Update*, *Domino Update*, *MQ Update*, *NT Update*, *Oracle Update*, *SQL Server Update*, and *TSO/ISPF Update*. Although the articles published are of a very high standard, the vast majority are not written by professional writers, and we rely heavily on our readers themselves taking the time and trouble to share their experiences with others. Many have discovered that writing an article is not the daunting task that it might appear to be at first glance.

They have found that the effort needed to pass on valuable information to others is more than offset by our generous terms and conditions and the recognition they gain from their fellow professionals. Often, just a few hundred words are sufficient to describe a problem and the steps taken to solve it.

If you have ever experienced any difficulties with RACF, or made an interesting discovery, you could receive a cash payment, a free subscription to any of our *Updates*, or a credit against any of Xephon's wide range of products and services, simply by telling us all about it. For a copy of our *Notes for Contributors*, which explains the terms and conditions under which we publish articles, please write to the editor, Fiona Hewitt, at any of the addresses shown on page 2, or e-mail her at fionah@xephon.com

Vanguard Enforcer is a new member of Vanguard's Quality Security Solution Suite, intended to automate the implementation, monitoring, and maintenance of corporate security policy for OS/390 Security Server (RACF) environments.

Enforcer's high level of security is based on proprietary technology first developed by the US National Aeronautics and Space Administration (NASA) in 1988. Vanguard has exclusively licensed and commercialized this technology from NASA.

For further information, contact:
Vanguard Integrity Professionals, 180 S. Anita Drive, Orange, CA 92868-3306, USA.
Tel: (714) 939-0377.
URL: http://www.go2vanguard.com

* * *

CONSUL has just released Version 2.2 of Consul/Enterprise Audit (CEA). New to this version is CEA/iView, a Web interface for auditing all components within an e-business environment from any workstation. It is compatible with both IE and Netscape Navigator, and uses an SSL connection.

CEA also includes improved audit analyses for Windows NT/2000, AIX, Sun Solaris, OS/390, Check Point FireWall-1, Cisco Router, and Microsoft IIS Webserver.

For further information, contact:
CONSUL Risk Management BV, Marshalllaan 2, 2625 GZ Delft, Netherlands.
Tel: (31) 15 2513333.
URL: http://www.consul.com
CONSUL Risk Management, 2840 Plaza Place, Suite 103, Raleigh NC 27612, USA.
Tel: (919) 782-3730.

* * *

EKC has introduced E-SME (Security Management Extension), a client/server API to maintain user IDs and the resources they can access. Through a TCP/IP connection, security modifications are performed under the administrator's user ID.

The latest release of the RACF tool ETF/R can perform dynamic class, router table, and exit updates without a system IPL.

For further information, contact:
Eberhard Klemens, 10400 West Higgins Road, Rosemont, IL 60018, USA.
Tel: (847)296-8010.
URL: http://www.ekcinc.com

* * *