27 RACF

February 2002

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

Code from *RACF Update*, and complete issues in Acrobat PDF format, can be downloaded from http://www.xephon.com/racf; you will need to supply a word from the printed issue.

Subscriptions and back-issues

A year's subscription to *RACF Update* (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. The price includes postage. Individual issues, starting with the August 1999 issue, are available separately to subscribers for £48.50 ($72.75) 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

When Xephon is given copyright, articles published in *RACF Update* are paid for at £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 or download a copy of our *Notes for Contributors* from www.xephon.com/nfc

Printed in England.

A REXX program to view USERID/GROUP access

I used to use IRRUT100 to obtain a list of profiles in which a USERID or GROUP existed. However, this approach didn't give me the access level that each Userid/Group had on that particular profile.

As I don't use the RACF DB2 tables, I decided to use the IRRDBU00 utility and DFSORT to get the results I needed. After I had the JCL to do it once, I decided it would be good to have a straightforward way of doing it, so I wrote a REXX program to format and submit the JCL, just passing the Userid/Group I wanted to check. Afterwards, it dawned on me that it would be even nicer to be able to pass several Userids/Groups in one run. That's how this program came to be written. It will produce an output file for each valid Userid/Group that it receives to check.

The program receives the Userid(s) and/or Group(s) to check, and discards any that aren't valid. It then gets the name of the RACF back-up database, by means of an RVARY, and formats and submits the JCL, which has four major blocks:

- DELETE
  - For each USERID/GROUP, a file will be allocated with

    ```
    DISP=(MOD,DELETE,DELETE),
    ```

    so that any old file, from a previous run, will be deleted.
- UNLOAD of the RACF back-up database
- SORT
  - This produces two temp files for each USERID/GROUP to check:
    - one for record type 0404 – Dataset Access
    - one for record type 0505 – General Resource Access.
- JOIN files
  - There will be an ICEGENER for each USERID/GROUP, joining the two temp files created by the SORT.

In the end, you will have a file for each USERID/GROUP, in which the last qualifier is the search argument:

```
userid.RACF.IRRDBU00.sysname.XXXXXXXX
```

Because the name, up to the last qualifier, is defined as a variable, it is easy to change, to adapt to different systems and different rules. The space units and quantities are also in variables, for the same reason.

The OUTPUT file will look something like this :

```
      DATASET  ALTER    Q1.Q2.**
FACILITY CONTROL  CICSF4
ACCTNUM  READ     123456
CONSOLE  ALTER    consname
STARTED  ALTER    STRBSM.*
```

SOURCE

```
/* rexx
                        ***********************
                        *                     *
                        *  Joao Bentes Jesus  *
                        *    SHOWACC 1.0.0    *
                        *                     *
                        ***********************
*/
parse upper arg all_data
if  all_data="" then
    do
        say"Error - No Group(s) and/or Userid(s) specified"
        say"        Program Interrupted"
    end
else
    do
        call check_all_data
    end
return
/* - - - - - - - - - - - - - */
check_all_data:
do  a=words(all_data) by -1 to 1
    prof=word(all_data,a)
    x=outtrap("ON")
    "LU ("prof")"
    if  rc=0 then
        x=outtrap("OFF")
    else
        do
            "LG "prof
```

```
            x=outtrap("OFF")
            if  rc=Ø then
                nop
            else
                do
                    all_data=delword(all_data,a,1)
                    say"ERROR - "prof" is not a valid userid/group"
                end
        end
end
wrds=words(all_data)
if  wrds>Ø then
    do
        call get_racf_dsn
    end
else
    do
        say"ERROR - There are no valid Userid(s)/Group(s) to check"
        say"        Program Interrupted"
    end
return
/* - - - - - - - - - - - - - */
get_racf_dsn:
x=outtrap(info.)
"RVARY"
x=outtrap("OFF")
if  rc=Ø then
    do
        racf_dsn=""
        do  a=1 to info.Ø
            if  word(info.a,1)="YES" &,
                    word(info.a,2)="BACK" then
                do
                    racf_dsn=word(info.a,words(info.a))
                    leave a
                end
        end
        if  racf_dsn\="" then
            do
                "ALLOC F("ddname") WRITER(INTRDR) SYSOUT(A)",
                    "LRECL(8Ø) RECFM(F)"
                if  rc=Ø then
                    do
                        call format_jcl
                    end
                else
                    do
                        say"ERROR ("rc") on Internal Reader Allocation"
                        say"      Program interrupted"
                    end
            end
```

```
        else
            do
                say"Error - Unable to obtain RACF backup data set name"
                say"        Program Interrupted"
            end
    end
else
    do
        say"Error ("rc") during RVARY execution"
        say"      Program Interrupted"
    end
return
/* - - - - - - - - - - - - - */
format_jcl:
sp_unit="TRK"
sp_prim=1Ø
sp_sec=5
root_dsn=userid()".RACF.IRRDBUØØ."mvsvar("SYSNAME")
job_name=userid()"I"
queue"//"job_name" JOB ('RACF'),'SHOW ACCESS',"
queue"//             CLASS=W,MSGCLASS=X,MSGLEVEL=(1,1),"
queue"//             REGION=32M,"
queue"//             TIME=144Ø,NOTIFY=&SYSUID"
queue"//*"
queue"//DELETE   EXEC PGM=IEFBR14"
do  a=1 to wrds
    z.a=right(a,2,"Ø")
    llq.a=word(all_data,a)
    mask.a=left(llq.a,9)
    queue"//"left(llq.a,8)" DD  DSN="root_dsn"."llq.a","
    queue"//             DISP=(MOD,DELETE,DELETE),"
    queue"//             SPACE=("sp_unit",("sp_prim","sp_sec"),RLSE),"
    queue"//             RECFM=VB,LRECL=4Ø96,BUFNO=2ØØ"
end
queue"//*"
queue"//IRRDBUØØ EXEC PGM=IRRDBUØØ,PARM=NOLOCKINPUT"
queue"//SYSPRINT DD  SYSOUT=*"
queue"//INDD1    DD  DISP=SHR,DSN="racf_dsn",BUFNO=2ØØ"
queue"//OUTDD    DD  DSN=&&WORK1,DISP=(NEW,PASS),"
queue"//             RECFM=VB,LRECL=4Ø96,BUFNO=2ØØ,"
queue"//             SPACE=("sp_unit",(75,75),RLSE)"
queue"//*"
queue"//SORTØ1   EXEC PGM=SORT,PARM='SIZE=MAX'"
queue"//SYSOUT   DD  SYSOUT=*"
queue"//SORTIN   DD  DSN=&&WORK1,DISP=(OLD,PASS)"
do  a=1 to wrds
    queue"//TØ4Ø4"z.a"  DD  DSN=&&TØ4Ø4"z.a",BUFNO=2ØØ,"
    queue"//             DISP=(NEW,PASS),"
    queue"//             SPACE=("sp_unit",("sp_prim","sp_sec"),RLSE),"
    queue"//             RECFM=FB,LRECL=8Ø"
    queue"//TØ5Ø5"z.a"  DD  DSN=&&TØ5Ø5"z.a",BUFNO=2ØØ,"
```



```
    queue"//             DISP=(NEW,PASS),"
    queue"//             SPACE=("sp_unit",("sp_prim","sp_sec"),RLSE),"
    queue"//             RECFM=FB,LRECL=80"
end
queue"//SYSIN    DD  *"
queue"  SORT FIELDS=COPY"
queue"  OPTION VLSHRT"
do  a=1 to wrds
    queue"  OUTFIL FNAMES=T0404"z.a",CONVERT,"
    queue"      INCLUDE=(5,4,BI,EQ,C'0404',&,62,9,BI,EQ,C'"mask.a"'),"
    queue"      OUTREC=(1:C'DATASET  ',10:71,9,19:10,52,10X)"
    queue"  OUTFIL FNAMES=T0505"z.a",CONVERT,"
    queue"      INCLUDE=(5,4,BI,EQ,C'0505',&,266,9,BI,EQ,C'"mask.a"'),"
    queue"      OUTREC=(1:257,9,10:275,9,19:10,62)"
end
queue"/*"
queue"//*"
do  a=1 to wrds
    queue"//JOIN"z.a"     EXEC PGM=ICEGENER"
    queue"//SYSPRINT DD  SYSOUT=*"
    queue"//SYSUT1   DD  DISP=(OLD,PASS),BUFNO=200,DSN=&&T0404"z.a
    queue"//         DD  DISP=(OLD,PASS),BUFNO=200,DSN=&&T0505"z.a
    queue"//SYSUT2   DD  DSN="root_dsn"."llq.a","
    queue"//             DISP=(NEW,CATLG,DELETE),"
    queue"//             SPACE=("sp_unit",("sp_prim","sp_sec"),RLSE),"
    queue"//             RECFM=FB,LRECL=80,BUFNO=200"
    queue"//SYSIN    DD  DUMMY"
    queue"//*"
end
zx=queued()
"execio "zx" diskw "ddname" (finis)"
if  rc\=0 then
    do
        say"ERROR ("rc") on Internal Reader WRITE"
        say"      Program Situation Unknown"
        say"     "queued()" of "zx" records",
            " were left on the Internal Reader"
        "dropbuf"
    end
else
    do
        zedsmsg="JOB "job_name" SUBMITTED"
        zedlmsg="RACF Access check for "all_data" has been submitted",
                "as "job_name
        address "ISPEXEC" "SETMSG MSG(ISRZ001)"
    end
"free f("ddname")"
return
/* - - - - - - - - - - - - - */
```

Joao Bentes de Jesus
Systems Programmer (Portugal)

RACF restructuring – part one: planning

This series of articles will provide the basis and technical processes to repair and restructure your RACF database. It's intended for IS managers and technicians who are conversant in RACF and OS/390, and who have a good project management background. For, make no mistake, this is not just a technical exercise. It can and should be a long-term and carefully planned project, involving staff from a variety of business and technical areas of your organization.

The series will be in four parts: planning, coding, testing, and implementation. These are described in turn below.

- *Planning* (this article) deals with the whys and wherefores of actually developing a RACF restructuring project for your organization. It looks at who should be included in the project, developing the initial analysis of your current database, and discusses tools and techniques that can help.
- *Coding* will look into the structure you wish to build into the new RACF database, both to correct old problems and to ensure future expansion and flexibility in the system. It will also look at a naming convention for groups and users which is most effective. There will be sections on creating a common structure for CICS, dataset, User and Group records, and time-saving tips on building the JCL.
- *Testing* will provide the templates for developing an initial (test) database, as well as insights into the problems and pitfalls you may encounter (and how to deal with them). It will review the building of your initial test LPAR, incorporating the new structures, and the phases of testing necessary to ensure a smooth development.
- *Implementation* will show how to convert the database from development to test to QC to Production without serious damage to your mental health.

WHY RESTRUCTURE?

The old adage, “if it ain’t broke, don’t fix it” is a common refrain when confronted with a major restructure of any database, and RACF is no exception. However, restructuring (or more accurately, rebuilding) your security database can become a necessity if you have an older database that has gone through several upgrades without making a significant review of the current structure.

If your company has gone through major internal (organizational) restructuring, the access requirements of your users will have changed as well. If your naming conventions are a mess (whether they be User ID, Group, General Resource, etc), restructuring gives you the opportunity to correct the mistakes of the past and build a foundation for an expandable and flexible system, while still providing the maximum level of security.

Here’s a general rule of thumb. If you haven’t taken a good long look at your RACF database or kept the structure up to date for more than four years, you should seriously consider restructuring.

WHEN TO RESTRUCTURE

Here are some specific reasons and time frames which should lead you to consider restructuring your RACF database:

- If your naming conventions for User IDs have changed, or haven’t been followed, over the past few years.
- If your naming conventions for Groups have changed.
- If your naming conventions for Datasets have changed.
- If you have replaced one or more major systems in the past few years.
- If your Group Tree doesn’t match your overall organizational structure (for the business side of mainframe access).
- If your Group Tree isn’t specific for the types of OS/390 and RACF accesses required by your organization.
- If your Group Tree doesn’t segregate organizational access from OS/390 and RACF access.

- If you have more Groups than User Ids.
- If your Dataset access structure is confused (or just confusing).
- If you provide access to Datasets, General Resource profiles, CICS Transactions, etc, by User ID and not by Group or Function.
- If you have more than 10 CICS regions defined in the database.
- If you note that your RACF database size is coming close to its limits (as determined through IRRUT200 analysis).
- If your RACF database BLKSIZE is not efficiently tailored to the maximum block size for the storage device it resides on. As a rule of thumb, BLKSIZE should be (TRACK SIZE / 2) / LRECL – to the nearest whole number. So, for example, on a 3390 track size of 56,664 bytes, and an LRECL of 4096, your BLKSIZE should be 24,576 (LRECL * 6.916 rounded to 6).
- If you're working with the default RACF structure provided initially by IBM.
- If the current database structure is similar to Marge Simpson's hairdo after intensive electroconvulsive therapy (see also: rat's nest).

If you have three or more of these indicators, you should perform a restructuring analysis, to determine the severity of the problem(s) and the potential benefits of restructuring in terms of system, operational, and administrative efficiency (see below).

WHEN NOT TO RESTRUCTURE

There are certain instances where restructuring is not an effective or efficient use of your resources. Note that they aren't just the opposite of "When to restructure", but there are elements that have similarity. You should NOT restructure the RACF database when or if:

- Naming conventions are in place across the board, and are enforced.
- Your Group Tree is designed in a tree shape (generally triangular), not like ground shrubs or a maypole (either too wide or too narrow).

- Your Group Tree adequately reflects the structure of your organization.
- Groups are segregated between organizational access and RACF – OS/390 access requirements.
- Access is provided to resources only by Group, not by User ID.
- You're not willing or able to allocate 12 to 18 months of time to the project.
- Your system doesn't have the capacity to create a separate LPAR (Logical PARtition) for development and testing of the restructured database.
- You don't have the full and complete support of upper management.
- You don't have the full and complete support of your business area managers or IT management.
- Your company's medical insurance won't cover the psychiatric treatment you'll require during and after the project.
- You have even a tenuous grip on sanity and reality.

BENEFITS AND PITFALLS

As with any major project (and restructuring the RACF database *is* major, make no mistake), there are benefits and drawbacks that must be considered. The benefit must outweigh the risk (as well as the cost), and must be a provable, long-term advantage to the system(s), to organizational security, and to the organization itself. The benefits must also be expansive (not expensive), including areas beyond the Information Security realm. If your organization has a quality control department and an internal audit function, and uses stringent change management and SDLC protocols, these are relatively easy to determine and illustrate to upper management and other involved parties. If you don't have those functions in your organization, you'll find it much more difficult (if not impossible) to obtain approval for such a major undertaking.

One important point: if your organization uses change management and SDLC protocols, make sure you follow these to the letter. Besides

cutting down on the complaints from those departments (and from internal and external auditors as well), you'll be greatly increasing your chances of project success. You'll also take care of those nasty jobs that nobody wants (ie documentation) during the project, instead of trying to develop everything at the last minute (if ever).

SELLING THE PROJECT

So, how can you sell a restructuring project to the various players: technical support, IT management, business management, and, most importantly, upper management (the ones with the money)? Use the three items that are guaranteed to sell any project: efficiency, greed, and fear. No, that's not a jaded viewpoint – it comes from many, many years of experience.

- Efficiency
  - Faster throughput of security-related calls within the operating system.
  - More efficient and effective use of database space (and disk space).
  - Easier and faster identification of Users/Groups/Datasets/Functions.
  - Fewer security violations on items needed by the business areas.
  - Better organization of system resources, based on standardized naming conventions.
  - Access based on organizational/departmental/unit/system requirements.
- Greed
  - Reduction in operational cost for security admin staff (fewer admin staff required to untangle or maintain a messy database).
  - Faster (ie cheaper) additions/changes/deletions of access.
  - Smoother processing due to reduction in 'false' or unintended security violations.

- Fear
  - Failure to restructure means gaps in security, where unauthorized users may abscond with sensitive corporate information.
  - Gaps in security can also mean unintentional alteration or deletion of data, which has costs in both time and money.
  - Loss of the RACF database in its current dishevelled state could cause loss of security data in the short run, and an expensive and time-consuming rebuild while slowing down production work.
  - Non-standard naming conventions can cause problems in access authorizations, as well as the removal of old or unused IDs/Groups/Datasets/Functions.

Of course, if you're developing a business case for a restructuring project, you won't want to use the headings above (management gets cranky about such things). You can summarize the project benefits and drawbacks as follows:

- Project benefits
  - More logical and standardized RACF database structures.
  - Greater operating system efficiency in RACF system calls and searches.
  - Immediate on-line identification of owners and authorizers of datasets, programs and other system resources, resulting in increased security.
  - Accurate on-line identification of users requesting password resets, resulting in greater security and efficiency.
  - Significantly reduced risk of user ID/password 'sharing' by staff.
  - Increased security over the selection of passwords by staff.
  - More accurate RACF reporting, both for IS security and for the owners and authorizers of datasets, programs, and other system resources.

  - Finer level of access control over resources, resulting in greater security and a significantly reduced risk of accidental or intentional alteration or deletion of important company information.
  - Easier to use, more informative input screens and panels for IS security, which will automatically enforce new naming conventions and standards.

- Project drawbacks
  - Long implementation period: project duration estimated at 9 to 12 months, including all analysis and management signoffs.
  - Increased initial maintenance requirements for IS security, estimated at roughly 5% for the first 12 months.
  - Some inconvenience to users during the transition periods for copying old JCL and files to new locations.
  - Increased responsibility on owners and authorizers of system resources to maintain control over their property (in this case, data). This is less of a drawback and more of an operational necessity.

PROJECT BASIS

The basis for any large-scale project is making sure the benefits (both short- and long-term) outweigh the disadvantages. As we saw above, using fear, greed, and efficiency can be helpful in creating an overall business case. I'm sure you can think of other items that are tailored to your organization.

Since this is such a large and wide-ranging project, you may be tempted to farm it out to a consulting firm. However, I'm a firm believer in doing as much of the work as you can on an in-house basis. Yes, you may need consultants here or there to provide additional expertise, or just an extra set of helping hands in coding, testing, and implementing the new database. However, outsourcing the entire project may not give you everything you want or need. Also, consultants are generally more costly (on a per hour basis) than your own staff, especially when they start charging overtime!

Ultimately, your restructuring project should be defined in phases:

1 Initial analysis.

2 Development of draft database.

3 Testing of draft database.

4 Conversion of development system database.

5 Testing and implementation of development system database.

6 Conversion of production system database.

7 Testing and implementation of production system database.

A phased approach will allow you better control over the tasks, as well as some effective kill points to keep the project from running out of control.

WHO TO INCLUDE AND WHY

Restructuring a RACF database cannot be done in a vacuum, with only the Information Security staff involved. That database, and any changes to it, are vital to every mainframe user, every production application, and every utility, function, dataset, and CICS transaction within the mainframe environment. You must therefore include the following people in the discussions, planning, and implementation of a restructuring project:

- *Upper management*. They're the ones who have to support this project from the get-go, so it's imperative to sell them on the benefits of restructuring. If you don't have the support of upper management, you don't have a project. Sell them early on, by developing a detailed business case showing the advantages of restructuring and the drawbacks of doing nothing.
- *IT senior management*. These are the folks who'll have to live with the consequences of your actions first-hand, especially when (not if) something crashes at 02:00 during a production cycle. Luckily for them (and for you) they only need monthly updates and don't get involved in the grunt work. However, they will hopefully be the ones supplying the budget for the project, and for any ancillary software packages you might need to make it work. Keep them

apprised, but don't overload them with too much information. (You'll know when that happens, from the gentle sound of snoring during any meetings with them.)

- *OS/390 technical support*. These people know the ins and outs of the system better than anyone else, and are also the ones who will find you the space for the testing LPAR you'll require. Be very *very* nice to these people, and heed well their advice and counsel. Never get on the bad side of your tech support staff – you'll come a cropper every time. Where possible, supply them occasionally with free doughnuts.

- *Change management*. Most organizations with even small-sized development teams have (or at least should have) a dedicated change management department. They should be involved to ensure that you've included all application systems (in development, test, QC, and production) as well as the CM software that controls these changes. They are quite valuable in the area of naming conventions (along with production support), and can be helpful in the early design phases as well as actual testing of the 'draft' database.

- *Production support*. The people who actually make the system run are a vital resource. They know what system feeds into which database, how long overnight batch processes should run (and in what order), and what changes can cause major headaches.

- *Quality control/quality assurance/quality management/quality etc*…. These people are experts at testing. And you will need to test the restructured database many times before it's ready to be promoted to a production environment. If there's a way to bring a system to a grinding halt, these folks will know about it. Use that knowledge to build redundancy into the new database. Failure in a test environment ultimately means success in a production one.

- *Internal audit*. The people you love to hate. The people who ask the annoying questions. The people who live and breathe 'control and exposure'. Internal audit (especially those of a technical bent) needs to ensure that controls are built in and exposures are minimized. Most likely, they will be in favour of fixing a database that isn't working well (or sometimes isn't working at all!). Keep

them involved at all times, and closely, and you'll find that your new database works a whole lot better. Also, if they help design it, they can't come back and complain about the design in subsequent audit reports. You should keep internal audit on your free doughnut list as well.

- *Business owners of key application systems*. Whenever there's an IT project, these are the people that are most often forgotten. However, they have a vested interest in the security of their systems. After all, they are the owners. They are a resource that should not be ignored, even if they don't know all of the technobabble. What they do know (or should know) is who may access their applications and their data. They may also know what their systems interface with (both internal and external to the mainframe). Keeping them in the loop, and taking their advice where possible, means a smoother transition. It also gives you the opportunity to 'sell' security to the user community. It is an opportunity you should not pass up.

INITIAL ANALYSIS

To know where you're going, you have to first figure out where you are. There are several ways to do this. The first analysis is quite simple using RACF-based tools. Run the IRRUT200 utility with the MAP and INDEX parameters first. This will give you a baseline of database size, structure, and potential overcrowding. Also run the IRRUT400 utility, but only for the reporting and not for the actual copy of the database. This will give you an indication of any potential problems in the structure of the database (although IRRUT200 is more comprehensive – this is just a double-check).

You should also run the DSMON report. This will give you the group tree structure. Map this structure out onto a flowcharting or organization charting software program (my personal preference here is Visio, but you can use any tool you like). This will take time, and it will seem like a meaningless exercise. But it does have an important purpose. It makes you keenly aware of the visual structure of the security groups within RACF, and that familiarity will help you in the design phase of the new database structure. The DSMON will also give you the STCs defined in the system. Match that against the STCs defined in OS/390 (your

tech support staff can help you here). Note any STCs that haven't been defined in RACF, and plan to include them.

While you're at it, you should generate a listing of all User IDs in the system. If you're so inclined, you can link those users to the Group Org chart (but this is time consuming, especially if you have a lot of users and/or groups to contend with). Once again, this gives you a level of familiarity, which is quite beneficial in your future work.

Generate CLISTs of all General Resource profiles, especially those involving FACILITY class settings. It's also prudent to take all of this information and generate it, if possible, into JCL for use in later database building. It will double as a back-up for correcting lost or deleted settings. Don't run them from the CLIST library, simply copy them to a PDS and download them to a text file. You'll find the information useful later.

Run a SETROPTS LIST and review the current settings. You may wish to make improvements or changes on this for the new database that may not be as feasible on your current one. Keep those in mind for your design work.

Once you have all of this information (and trust me, it's not a small amount), you should then try to find the gaps – the items that aren't covered by all of the profiles in the system. If you have your RACF database set in FAIL mode, this may seem to be a waste of time. It is not. Your goal is to ensure that you've covered all of the systems, data, users, and facilities so that they are explicitly defined. Also, remember that FAIL mode can be overridden in certain instances, so it's a better plan to try to cover all contingencies.

Now for the fun part. Go to your Human Resources department and get a detailed copy of your company's organization chart, a list of all current employees, a list of all current contractors and temporary staff, and (if possible) a list of key management personnel. Sounds like a simple task, but trust me, it isn't! Odds are, if you ask for this information, their first response will be "Huh?". If they do have this information readily available, you'll need it for a number of different tasks. The organization chart will be used to develop your new RACF group structure – well, half of it, anyway. You'll see what I mean in the next instalment. Take the list of employees, contractors, and temporary

staff, and compare it with the list of all the RACF users. You'll probably find a number of old IDs that don't correspond to your current staff list. Take this opportunity to remove them from the current RACF database.

Now check with your contacts in technical support and production control. They should have a listing of all the Started Task jobs. Cross-reference those STCs with the User ID list as well. You'll need to keep those IDs, and their associated access authorities, in the new database. Don't worry if those names don't match the new naming conventions you're planning to use. They'll stand out as glaring exceptions, which will make them much easier to identify when you run a general ID listing in the future.

Also, see if technical support can give you a listing of utility software that's used on a regular basis. Make a special effort to identify what those utilities require in the way of secured access.

Once you've completed the analysis, you'll have a good understanding of your current system. You'll also have a handle on whether you need to proceed to actually restructuring the database, or if you can get away with doing corrective maintenance to plug up some of the holes. If you find that your system isn't as badly mangled as you originally thought, congratulations. You can save yourself a lot of strenuous effort. If you find, however, that your system is even worse off than you first feared, welcome to the club! I've found that most shops that actually take the time and effort to do the initial analysis end up more in the latter group than in the former. Sad, but true.

TOOLS AND TECHNIQUES

The items above mainly mention IBM utilities already bundled into RACF. These are okay, but only up to a point. Let's face it, IBM didn't exactly put a lot of time and effort into its reporting and input systems for RACF. We've all had to deal with the nightmare that is RACFRW, after all. There are other tools you can use to not only help your analysis, but also in some cases to actually perform the conversion.

Two of the most popular multi-function systems are Consul/RACF+Audit and Vanguard QS/390 with RioVision. Both of these packages are quite good, and offer a great deal of flexibility and

usability in RACF administration, analysis, and reporting. They also offer something that RACF should offer – cloning and renaming of IDs, Groups, General Resource Profiles, etc.

If you don't have either of these packages, I strongly suggest that you review them both. Do a comparison of the functionality and capabilities, and decide which one is best for your organization. I'm not recommending one over the other (although I've worked with both and I think they are excellent products) mainly because different companies and security departments have different needs and priorities. The cost savings either product will provide more than make up for the initial cost. They're also really easy to install, easy to use, and their documentation is first rate:

- Vanguard

  http://www.viplink.com/products/Vanguard_Security_Suite.cfm

- Consul

  http://www.consul.com

If you find that your organization can't justify the expenditure in the current financial environment, there are some freebies that will help you with the analysis. They won't help as much with the actual conversion, but they'll at least give you the up-front help you'll need to see just how deep a hole you're actually stuck in.

IBM has a couple of freebies, such as DFSORT/ICETOOL and IRRUT100, which offer some extended reporting capabilities. IRRUT100, IBM's cross-reference facility, is a bit of a bear to run, especially if you're trying to do an analysis of an entire system. Also, it will tell you what a User ID or Group is connected to, but it doesn't tell you what the authority level is, which is a bit of a pain.

IBM also has a Redbook, which details the use of its "OS/390 Security Server Audit Tool and Reporting Application" (SG24-4820-00), available at http://www.redbook.com. The tool components can be downloaded from ftp://lscftp.pok.ibm.com/pub/racf/mvs/os390art, and there are also a number of on-line reports that are quite good.

My personal favourite, however, is a collection of PC-based utilities created by Nigel Pentland. There are 60+ utilities which can list User

IDs, Groups, and General Resource profiles, as well as perform cross-reference and analysis functions much better than IBM. It can even report on OMVS allocation (which IBM's reporting facilities can't). It requires you to download the RACF database to a flat text file using the IRRDBU00 facility, but it is well worth the effort. And it's at a price your budget office will love – it's FREE! You can download the stuff you need from http://www.cairnleck.co.uk/nigel/racf.htm. I'll discuss which of the utilities are most useful in the next article.

IN OUR NEXT EXCITING EPISODE...

- *Thrills* when you begin the task of building a new Group structure!
- *Chills* when you see just how large a task that is!
- *Spills* when you dump your coffee cup over your terminal in frustration!
- *Pills* for calming your nerves!
- *Gills* for swimming in the ocean!

Okay, seriously. The next instalment in this series of articles (next issue) will present a new, and hopefully more logical, Group structure as well as advice on User ID and CICS resource naming conventions. It will segregate groups into two main structures: organizational (based on your company's organization chart) and system (which segregates RACF and OS/390 functions into a hierarchy). You'll see how this structure can be much more efficient and effective in controlling system security.

Part two will also give hints and tips on generating the JCL by using MS Word. It's a neat trick that can save you several hours of repetitive and mindless keyboard work, and cuts down on the errors that invariably crop up during coding.

We'll also examine (for the more advanced or adventurous) the rebuilding of RACF ISPF input and display screens into something a bit more formatted and functional.

And there'll be hints and tips on how to best create your test LPAR, the general size requirements, and advice on the order of building the

database from the JCL you've created, and on how to do the initial database configuration.

Doc Farmer
Manager and Senior IS Security Analyst (Middle East)

(Doc Farmer would welcome comments and suggestions on this article. He can be contacted at Doc.Farmer@sbm.net.sa)

Inside IBM – RACF and security since October 2000

For most of the 1990s, I wrote a monthly column called 'Inside IBM', which contained technical summaries of recent IBM mainframe announcements. This article is constructed along similar lines, and summarizes the security-related changes in z/OS, z/VM, and the 2064 eserver zSeries 900 (z900) hardware since they were first announced on 3 October 2000.

RACF

Well before z/OS, RACF had already become a component of SecureWay Security Server, along with Distributed Computing Environment (DCE) Security Server, Lightweight Directory Access Protocol (LDAP) Server, and z/OS Firewall Technologies. Security Server is an optional separately priced feature of z/OS. Elements and optional features of z/OS are tested together for compatibility by IBM.

Nonetheless, RACF can be obtained as a stand-alone software product, typically to upgrade an older OS/390 environment with a newer version of RACF. For VM, RACF remains (solely) a stand-alone product. All releases of z/VM run only one release of RACF (5740-XXH): Version 1 Release 10.0. On a z900, APAR VM62598 is required (technically only when running in 64-bit mode).

Z900

The z900 replaced the entire System/390 line of mainframes, both the 9672 Parallel Enterprise Servers Generation 6 (G6) and 7060 Multiprise 3000.

The z900 CMOS Cryptographic Coprocessor uses faster technology than its System/390 counterpart on a single-chip module that is mounted right on the processor board. Up to two are standard equipment on the z900. The 4758 PCI Cryptographic Coprocessor (PCICC) increases performance and adds function. Up to eight PCICC features can be installed, but each feature is actually two PCICCs. Load balancing allows 2000 Secure Socket Layer (SSL) transactions per second to be processed with 8 PCICC features installed and 2 CMOS Cryptographic Coprocessors active.

Z/OS 1.1

Version 1.1 of z/OS replaced OS/390 (which replaced MVS/ESA), further expanding the integration of separate software products into the operating system.

Elements are the software components that come with z/OS. Technically, it's possible to have IBM remove a few of them, and perhaps save a little money, but doing so voids IBM's integration testing warranties. The elements that are related to security include:

- Cryptographic services
  - Integrated Cryptographic Service Facility (ICSF) supports hardware encryption functions, including Triple Data Encryption Standard (DES), on 9672 G5 and G6, z900 and Multiprise 3000 servers.
  - Open Cryptographic Services Facility (OCSF).
  - System SSL.
- Communications server
  - SNA/Advanced Peer-to-Peer Networking (APPN) Services, of which VTAM is a part, includes limited DES.
  - TCP/IP Services, of which TCP/IP for MVS is a part, includes Firewall Commercial Data Masking Facility (CDMF) 40-bit, Version 3 of Simple Network Management Protocol (SNMPv3) DES 56-bit, and IPSec (Internet Protocol Security) DES 56-bit.

- LAN services
  - LAN Resource Extension and Services (LANRES) includes limited DES.
- Systems management and security
  - Tivoli Management Framework for z/OS includes limited DES 56-bit.
- Distributed computing services
  - DCE Base Services includes limited DES.
  - Distributed File Service, includes DES 56-bit.
- Application Enablement Services
  - Language Environment includes limited DES.
- Unix System Services (USS or Unix).

Optional features are those components of z/OS that are priced separately. In the security-related list below, Level 2 provides DES and Level 3 provides Triple DES:

- SecureWay Security Server
  - RACF
  - Network authentication and privacy service
  - LDAP server
  - DCE security server
  - Firewall technologies
  - Open cryptographic enhanced plug-ins, which uses OSCF.
- Cryptographic services
  - OSCF security level 3
  - System SSL security level 3.
- Communications Server (CS)
  - CS security level 1

  - CS security level 2
  - CS security level 3.
- e-business services
  - IBM HTTP server North America (NA) secure.
- Systems management
  - Resource Measurement Facility (RMF).

SecureWay Security Server

Although the SecureWay Security Server is listed as a z/OS optional feature, its Network authentication and privacy service is actually an element that's included with z/OS.

The z/OS SecureWay Security Server RACF collection is orderable as SK3T-4272 or Feature Number 8001 of z/OS. It includes both BookManager and Adobe Acrobat (.pdf) versions of unlicensed SecureWay Security Server manuals, RACF-related redbooks, flyers, education course listings, and sample code. It replaces the OS/390 SecureWay Security Server RACF Information Package (SK2T-2180).

Z/OS 1.2

The new features and enhancements in z/OS Version 1.2 are described below.

SecureWay Security Server

RACF

In z/OS 1.2, RACF-defined users can be given authorization to request a client digital certificate through a Web-based application and have it downloaded to the user's Web browser. This function is also available through RACF and System Authorization Facility (SAF) Authorized Program Analysis Reports (APARs) to z/OS 1.1 and OS/390 2.10.

In z/OS 1.2, a RACF Universal group can have an unlimited number of

users. It's intended for use with e-business applications where large numbers of users are often needed.

RACF messages were improved for security failures while accessing Unix files and directories. Superuser granularity was extended to cover the Unix chmod command.

In z/OS 1.2, Coupling Facility (CF) errors are less likely to cause RACF failures. Security tracing was also improved.

Network Authentication and Privacy Service

Network Authentication Service for z/OS is a stand-alone Kerberos Version 5 implementation that does not require DCE and was originally added to OS/390 Security Server. It provides both a native Kerberos Application Programming Interface (API) and the Internet standard Generic Security Service (GSS) API.

New with z/OS Version 1.2 were the following:

- New ways to administer Kerberos registry information outside of z/OS.
- Stronger encryption.
- Use of the cryptographic coprocessors.
- Increased availability across TCP/IP network outages.
- Improved performance in parallel sysplex.

LDAP

In z/OS 1.2 LDAP is Entrust-certified. Both its directory client and server support Kerberos. The LDAP server now supports thousands of concurrent clients, instead of hundreds. It can be configured to listen on a specific interface/port combination. There was also an LDAP Configuration Utility that automates a basic set-up.

For increased security, z/OS 1.2 allows Kerberos credentials to be used to bind LDAP servers, whether they reside on or off z/OS. Client-side caching of search results makes some LDAP searches run faster. An LDAP server can be found with information in a Domain Name System (DNS) server without prior knowledge of the LDAP server's host name or IP address.

SDBM created an access method for LDAP using RACF's internal database; it provides the capability to manage RACF-defined users and groups using the LDAP protocol. Like Unix, SDBM is not actually an acronym because each letter does not equate to a word. SDBM started life as RDBM plus one (R + 1 = S). RDBM uses DB2.

In z/OS 1.2, SDBM includes support for connection profiles (adding users to groups), the Kerberos segment, the Lotus Notes segment, and the Novell Directory Services (NDS) segment.

Firewalls Technologies

Internet Key Exchange (IKE) Commit Bit support was new in z/OS 1.2. Configuration of dynamic Virtual Private Networks (VPNs) was added to the Firewall Graphical User Interface (GUI) in the form of a dialogue that leads you through the process. The Internet Security Architecture Key Management Protocol (ISAKMP) server can also detect the presence of a Virtual IP Address (VIPA) on a firewall stack when that stack acquires the VIPA.

Cryptographic services

The PCICC has supported the loading of customized cryptographic functions for some time. OS/390 2.10 added support (User-Defined Extensions), but you had to have IBM build them for you. With z/OS 1.2, you can contract with IBM to write them yourself.

System SSL

In z/OS 1.2, System SSL supports Transport Layer Security (TLS), Public Key Infrastructure for X.509-compliant Certificate Revocations Lists (PKIX CRLs) created by Tivoli SecureWay Public Key Infrastructure, application creation of multiple SSL environments within a single process, and interactive debugging. System SSL detects a severed connection to the LDAP server and re-establishes the connection, removing the need for applications to re-establish SSL sessions after an LDAP server is recycled. System SSL also detects changes in the RACF key ring, through an Application Programming Interface (API) that indicates modifications have occurred since the SSL environment was defined.

Communications Server

With z/OS 1.2, Kerberos Version 4 support was removed from Communications Server, in favour of Kerberos Version 5 already in z/OS. Communications Server components upgraded to use z/OS built-in Version 5 support include the following:

- USS Telnet Server allows clients to log in to the USS shell environment using Kerberos as the authentication protocol.
- FTP client and server support Kerberos through GSS-API Version 2.
- USS RSH server can be configured to support RSH (Remote SHell, a Unix command) clients supporting Kerberos directly or via the GSS API.

The Express Logon Feature (ELF) allows anyone with a tn3270 (telnet 3270) client session and X.509 certificate to log on to a z/OS-based SNA application (such as CICS, TSO, or IMS TM) without a user ID or password. The process uses the RACF PassTicket supported by Version 5 of Host On-Demand (HOD).

The tn3270 server's Enhanced Logical Unit (LU) mapping support for dynamic IP environments allows the definition of rules that assign LUs for clients that are assigned dynamic IP addresses. The most practical application is for tn3270e (telnet 3270 extended) clients using dynamic IP and attempting to establish a tn3270e SSL-protected session. The tn3270e server queries RACF with the client's certificate to obtain the user ID, then assigns an LU based on that user ID and an LU assignment policy defined to the server.

A security policy can be used to control the use of the netstat command in both TSO and USS shell environments. Selected options of the command can be controlled on a per-user basis.

The SNMP subagents permitted to connect to an SNMP agent running the same z/OS image can be controlled using SAF interfaces. Policies can be defined in profiles with RACF and competitive products.

IP routing has enhanced security when using Open Shortest Path First (OSPF) dynamic routing protocol. When users specify Message Digest (MD5) authentication of OSPF updates, the OMPROUTE routing

daemon will verify that routing updates are received only from authenticated routers within the network. This also allows z/OS to be part of the same OSPF area as other routers that support MD5.

The Simple Mail Transfer Protocol (SMTP) server provides an exit for spam control. A sample Assembler exit is provided that examines incoming mail before processing. The exit receives control for most SMTP data flows, including SMTP command processing and actual data transfers.

FTP

The FTP Client and Server of Communications Server both support SSL and TLS. This provides encryption, authentication, and message integrity services for the FTP control and data connections. Optionally, an FTP client-provided X.509 certificate that's authenticated during the SSL/TLS handshake can be used for end user identification and authentication in addition to user ID and password verification.

The FTP client also supports SOCKS protocols, allowing it to directly connect to Internet FTP servers through the many firewalls that implement TCP connection relay functions in the form of SOCKS servers.

To prevent bounce attacks when the FTP server is used as an Internet FTP server, configuration options control the use of the PORT FTP command, either disabling it or restricting its use. Bounce attacks see FTP clients misusing the passive transfer mode of the FTP protocol to re-route a data connection.

IDS

In z/OS 1.2, Intrusion Detection Services (IDS) is integrated with the z/OS Communications Server stack. Intended to protect z/OS, it focuses, though not solely, on what an external network-based intrusion detection system cannot do – such as examining data after decryption that IPSec end-to-end encryption prevented the external intrusion detection system from evaluating.

IDS can discard attacking packets before they cause damage, discard packets exceeding established thresholds, and limit the number of connections from greedy users. IDS provides event recording and

reporting, including standalone reporting of IDS events (attacks) to the eserver z900 console and System Log file (SYSLOG). There's also a packet trace for off-line analysis, and statistics gathering for baseline and exception reporting.

Significant overhead is avoided by integrating the attack detection probe into existing error detection logic, rather than performing per packet examination against a table of signatures for many known attacks. Statistical anomalies are detected in real-time because it's easier for the target system (z/OS) to keep stateful data, internal thresholds, and counters.

IDS policies are kept in LDAP and can be triggered by scans, single packet attacks, and flooding. Actions include packet discard, connection limiting, and reporting. Log files and/or the console can receive event and statistical reporting.

Systems Management

RMF

In z/OS 1.2, performance reporting on cryptographic processing is shown by Crypto Using and Delay values in the Postprocessor WLMGL report. The Postprocessor Cryptographic Hardware Activity report provides performance monitoring for the use of PCICCs on an LPAR basis using SMF records type 70 subtype 2.

Z /OS 1.3

The new features and enhancements in z/OS Version 1.3 are described below.

SecureWay Security Server

PKI

PKI (Public Key Infrastructure) is a new transaction security and integrity component of SecureWay Security Server that is embedded in z/OS. PKI is a Certificate Authority (CA) that provides digital credentials, and a public-key cryptographic system that uses the credentials to help

ensure overall message integrity, signature verification, and user authentication. A Web interface can be used to generate (and manage) digital certificates for both RACF users and external clients.

Cryptographic Services

ICSF supports Public Key Cryptography Standards #1 (PKCS #1) Version 2.0 Optimal Asymmetric Encryption Padding (OAEP) Method of Key Encryption callable services. The same support can be added to ICSF in z/OS 1.2 and OS/390 2.10 through APARs, but there are also microcode release level requirements for the PCICC.

In z/OS 1.3, ICSF has increased its support of:

- Smart cards.
- The VISA, Zentraler Kreditausschuss (ZKA), and Europay banking standards.
- International standards for Personal Identification Number (PIN) processing and message authentication.
- The RSA (Rivest-Shamir-Adleman) *de facto* public key algorithm standard.
- National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) algorithm.
- The Derived Unique Key Per Transaction (DUKPT) algorithm.

The Public Key Algorithm (PKA) Key DataSet (PKDS) can also be re-enciphered when the PKA master keys are changed, rather than having to create an entirely new PKDS, as was previously required.

Unix System Services

In z/OS 1.3, both RACF and USS allow the use of Access Control Lists (ACLs) to add extended permissions to individuals and groups. ISHELL, a 3270 panel interface to USS, can be used to view and manage ACLs. Going beyond permission bits on a file, USS allows file access to be defined for a given user without allowing everyone else access or setting up a special group just for that user.

Z/VM 3.1

In Version 3.1, an SSL server has been added to the TCP/IP feature of z/VM; it requires Linux for System/390 to run. Installations define the ports where SSL will be provided, known as secure ports, and the certificates to be used. No changes are required to any VM servers listening on a secure port; SSL connections are automatically established with any external client that supports SSL. Encryption is supported in 40-, 56-, and 128-bit.

The Kerberos DES feature is now a part of the TCP/IP feature of z/VM. It provides 128-bit encryption/decryption services for the Kerberos authentication server as well as APIs for application programs.

z/VM 4.1

Support for the DCE User Data Privacy Feature, as well as DCE itself, ended with z/VM 4.1.

z/VM 4.2

In z/VM 4.2, TCP/IP stack security prevents some Denial of Service (DoS) attacks, including those known as Smurf, Fraggle, and Ping-o-Death: Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) Echo Request packets sent to IP broadcast or multicast addresses, and ICMP Echo Request packets that are too large.

CONCLUSION

This article has reviewed the security-related changes to z/OS, z/VM, and eserver zSeries (z900) since they were announced sixteen months ago. Given the sudden interest in security as a result of recent political events, you should expect more, not fewer, changes in the year ahead.

Jon E Pearkins
(Canada)

Consulting RACF with SQL

It's a challenge for RACF administrators to obtain sophisticated information about the objects residing in the RACF database. The traditional interface between RACF and its manager offers no way to make the relevant requests, and although it would make sense to use SQL, the RACF database is not a DB2 database. It's also difficult to read the SMF records generated by the usage of system tasks under the control of RACF.

This article describes an IBM facility which can be used to consult RACF data in a more user-friendly way than through the 3270 RACF interface, and which can also provide information which can't be obtained using native RACF tools.

TRANSFERRING RACF DATA INTO A DB2 DATABASE

First, we need to create a container which is OS/390 release dependent. You can do this as follows:

- Create the DB2 tables using standard DB2 DDL, adapted from member RACDBUTB in SYS1.SAMPLIB. The result is:
  - One database (by default named RACFDB2).
  - One multitable tablespace (by default named IRRDBU00). This tablespace can be altered for compression (parameter COMPRESS YES) and segmentation:

```
CREATE TABLESPACE IRRDBU00 IN RACFDB2
        USING STOGROUP RACFDB2
              PRIQTY   80000
              SECQTY   8000
              ERASE    YES
       FREEPAGE       0
       PCTFREE        0
       SEGSIZE        64
       BUFFERPOOL     BP8
       LOCKSIZE       ANY
       LOCKMAX        SYSTEM
       LOCKPART       NO
       CLOSE          NO
       COMPRESS       YES
;
```

Type	Table Name	Record Name
0100	GROUP_BD	Group Basic Data
0101	GROUP_SUBGROUPS	Group Subgroups
0102	GROUP_MEMBERS	Group Members
0103	GROUP_INSTALL_DATA	Group Installation Data
0110	GROUP_DFP_DATA	Group DFP Data
0120	GROUP_OMVS_DATA	Group OMVS Data
0130	GROUP_OVM_DATA	Group OVM Data
0140	Reserved	No non-repeat fields
0141	GROUP_TME_ROLE	Group TME Role
0200	USER_BD	User Basic Data
0201	USER_CATEGORIES	User Categories
0202	USER_CLASSES	User Classes
0203	USER_GROUPS	User Group Connections
0204	USER_INSTALL_DATA	User Installation Data
0205	USER_CONNECT_DATA	User Connect Data
0206	USER_RRSF_DATA	User RRSF Data
0207	USER_CERT_DATA	User Cert data
0210	USER_DFP_DATA	User DFP Data
0220	USER_TSO_DATA	User TSO Data
0230	USER_CICS_DATA	User CICS Data
0231	USER_CICS_OPCLASS	User CICS Operator Classes
0240	USER_LANGUAGE_DATA	User Language Data
0250	USER_OPERPARM_DATA	User OPERPARM Data
0251	USER_OPERPARM_SCOP	User OPERPARM Scope
0260	USER_WORKATTR_DATA	User WORKATTR Data
0270	USER_OMVS_DATA	User OMVS Data
0280	USER_NETV_DATA	User NETV Data
0281	USER_NETV_OPCLASS	User NETV Operator Classes
0282	USER_NETV_DOMAINS	User NETV Domains
0290	USER_DCE_DATA	User DCE Data
02A0	USER_OVM_DATA	User OVM Data
02B0	USER_LNOTES_DA	User LNOTES Data
02C0	USER_NDS_DATA	User NDS Data
0400	DS_BD	Data Set Basic Data
0401	DS_CATEGORIES	Data Set Categories
0402	DS_COND_ACCESS	Data Set Conditional Access
0403	DS_VOLUMES	Data Set Volumes
0404	DS_ACCESS	Data Set Access
0405	DS_INSTALL_DATA	Data Set Installation Data
0410	DS_DFP_DATA	Data Set DFP Data
0420	Reserved	No non-repeat fields
0421	DS_TME_ROLE	Data Set TME Role
0500	GENR_BD	General Resource Basic Data
0501	GENR_TAPE_VOLUMES	General Resource Tape Volume Data
0502	GENR_CATEGORIES	General Resource Categories

Figure 1: RACF record types (part one)

```
Type    Table Name          Record Name
----    ------------------- ----------------------
Ø5Ø3    GENR_MEMBERS        General Resource Members
Ø5Ø4    GENR_VOLUMES        General Resource Volumes
Ø5Ø5    GENR_ACCESS         General Resource Access
Ø5Ø6    GENR_INSTALL_DATA   General Resource Installation Data
Ø5Ø7    GENR_COND_ACCESS    General Resource Conditional Access
Ø51Ø    GENR_SESSION_DATA   General Resource Session Data
Ø511    GENR_SESSION_ENT    General Resource Session Entities
Ø52Ø    GENR_DLF_DATA       General Resource DLF Data
Ø521    GENR_DLF_JOB_NAMES General Resource DLF Job Names
Ø53Ø    (Reserved)
Ø54Ø    GENR_STDATA_DATA    General Resource STDATA Data
Ø55Ø    GENR_SVFMR_DATA     General Resource SVFMR Data
Ø57Ø    GENR_TME_DATA       General Resource TME Data
Ø571    GENR_TME_CHILDREN   General Resource TME Children
Ø572    GENR_TME_RESOURCE   General Resource TME Resource
Ø573    GENR_TME_GROUP      General Resource TME Group
Ø574    GENR_TME_ROLE       General Resource TME Role
Ø56Ø    GRCERT_DATA         Certificate Data
Ø561    CERTR_DATA          Certificate References Data
Ø562    KEYR_DATA           Key Ring Data
----    AUTH_IDS            Authorization Ids
```

Figure 2: RACF record types (part two)

  - 63 tables and 116 indexes (the default creator is USER01). Every table receives a specific RACF record type, as shown in Figures 1 and 2.

- Unload the RACF database using the IRRDBU00 utility. This can be done using the job shown below, and the result is in a format that can be viewed directly, processed by an application program, or, as here, uploaded to DB2. Clearly, then, there's really an enormous amount of very structured information (but no passwords!) within DB2 tables.

```
//DBUNLD   JOB  'DBA',CLASS=W,MSGCLASS=X,NOTIFY=&SYSUID.
//*
//IRRDBUØØ EXEC PGM=IRRDBUØØ,PARM='NOLOCK'
//SYSPRINT DD  SYSOUT=*
//INDD1    DD  DISP=SHR,DSN=USERØ1.RACF.DATABASE     racf database
//OUTDD    DD  DISP=SHR,DSN=USERØ1.RACF.IRRDBUØØ     datafile
//             UNIT=339Ø,SPACE=(CYL,(2Ø,5)),
//             DCB=(RECFM=FB,LRECL=4Ø96,BLKSIZE=Ø),
//             DISP=(NEW,CATLG,DELETE)
//SYSUDUMP DD  SYSOUT=*
```

- Reload the RACF data using the standard DB2 LOAD utility, with the SYSIN from the sample RACDBULD member in the SYS1.SAMPLIB. This utility contains one statement 'INTO TABLE' by table, and gives good performance for loading, because the data file (with the IRRDBU00 ddname) is read just once at the start of the job.

```
LOAD DATA
   INDDN IRRDBU00
   RESUME NO REPLACE
   LOG    NO
   INTO TABLE USER01.GROUP_BD
   WHEN(1:4)='0100' (
      GPBD_NAME            POSITION(006:013)   CHAR(8),
      GPBD_SUPGRP_ID       POSITION(015:022)   CHAR(8),
      GPBD_CREATE_DATE     POSITION(024:033)   DATE EXTERNAL(10),
      GPBD_OWNER_ID        POSITION(035:042)   CHAR(8),
      GPBD_UACC            POSITION(044:051)   CHAR(8),
      GPBD_NOTERMUACC      POSITION(053:053)   CHAR(1),
      GPBD_INSTALL_DATA    POSITION(058:311)   CHAR(254),
      GPBD_MODEL           POSITION(314:357)   CHAR(44)
      )

  INTO TABLE USER01.GROUP_SUBGROUPS
  WHEN(1:4)='0101' (
     GPSGRP_NAME          POSITION(006:013)   CHAR(8),
     GPSGRP_SUBGRP_ID     POSITION(015:022)   CHAR(8)
     )

  INTO TABLE USER01.GROUP_MEMBERS
  WHEN(1:4)='0102' (
     GPMEM_NAME           POSITION(006:013)   CHAR(8),
     GPMEM_MEMBER_ID      POSITION(015:022)   CHAR(8),
     GPMEM_AUTH           POSITION(024:031)   CHAR(8)
     )
```

..... continue for all the tables in a similar vein.

At our site, the RACF tablespace is compressed to 64%, and uses less than 2,000 tracks. The jobs last several minutes and the history and refresh frequency of the database are based on necessity.

IBM also gives some sample SQL requests. See member RACDBUQR in SYS1.SAMPLIB, and the appendices at the end of this article for some REXX which uses the standard REXX/DB2 interface.

Some of the members in SYS1.SAMPLIB can help to obtain information from a DB2 database:

- *Member IRRADUTB*. Creating the second tablespace IRRADU00 and its 70 tables (see Figures 3 and 4).

```
Table name         Event description
------------------ ------------------------------
JOBINIT            Job initiation
ACCESS             Resource access, other than file directory
ADDVOL             ADDVOL/CHGVOL
RENAMEDS           Rename dataset
DELRES             Delete resource
DELVOL             Delete volume
DEFINE             Define resource
ADDSD              ADDSD command
ADDGROUP           ADDGROUP command
ADDUSER            ADDUSER command
ALTDSD             ALTDSD command
ALTGROUP           ALTGROUP command
ALTUSER            ALTUSER command
CONNECT            CONNECT command
DELDSD             DELDSD command
DELGROUP           DELGROUP command
DELUSER            DELUSER command
PASSWORD           PASSWORD command
PERMIT             PERMIT command
RALTER             RALTER command
RDEFINE            RDEFINE command
RDELETE            RDELETE command
REMOVE             REMOVE command
SETROPTS           SETROPTS command
RVARY              RVARY command
APPCLU             APPC session
GENERAL            General purpose
DIRSRCH            Directory search
DACCESS            Check access to a directory
FACCESS            Check access to file
CHAUDIT            Change audit options
CHDIR              Change current directory
CHMOD              Change file mode
CHOWN              Change file ownership
CLRSETID           Clear SETID bits for a file
EXESETID           EXEC with SETUID/SETGID
```

Figure 3: Creating the second tablespace and its 70 tables (part one)

```
GETPSENT           Get process entry
INITOEDP           Initialize OpenEdition process
TERMOEDP           OpenEdition process complete
KILL               Terminate a process
LINK               LINK
MKDIR              Make directory
MKNOD              Make node
MNTFSYS            Mount a file system
Table Name         Event description
------------------ ------------------------------
OPENFILE           Open a new file
PTRACE             PTRACE authority checking
RENAMEF            Rename file
RMDIR              Remove directory
SETEGID            Set effective GID
SETEUID            Set effective UID
SETGID             Set GID
SETUID             Set UID
SYMLINK            SYMLINK
UNLINK             UNLINK
UMNTFSYS           Unmount file system
CHKFOWN            Check file owner
CHKPRIV            Check privilege
OPENSTTY           Open slave TTY
SETGROUP           SETGROUP
RACLINK            RACLINK COMMAND
IPCCHK             IPCCHK
IPCGET             IPCGET
IPCCTL             IPCCTL
CKOWN2             CKOWN2
RACFINIT           RACF initialization information
CLASNAME           Class information
DSNSAFF            Data sets affected by a SECLABEL change
ACCR               Access Rights Passed
RACDCERT           RACDCERT COMMAND
INITACEE           initACEE callable service
```

Figure 4: Creating the second tablespace and its 70 tables (part two)

- Extracting the RACF SMF records. This job can run daily.

```
//SMFUNLD   JOB  'DBA',CLASS=W,MSGCLASS=X,NOTIFY=&SYSUID.
//*
//SMFDUMP  EXEC PGM=IFASMFDP
//SYSPRINT DD  SYSOUT=A
//ADUPRINT DD  SYSOUT=A
//OUTDD    DD  DISP=SHR,DSN=USERØ1.RACF.IRRADUØØ
//SMFDATA  DD  DISP=SHR,DSN=USERØ1.RACF.SMFDATA.DØ10829
```

```
//SMFOUT   DD  DUMMY
//SYSIN    DD  *
     INDD(SMFDATA,OPTIONS(DUMP))
     OUTDD(SMFOUT,TYPE(000:255))
     ABEND(NORETRY)
     USER2(IRRADU00)
     USER3(IRRADU86)
/*
```

- Member IRRADULD. Loading the data.

SUMMARY

As we've seen, the non-user-friendly RACF 3270 interface can be replaced, for reading, by an ordinary SQL tool such as SPUFI, QMF, or similar. What's more, extra information can be retrieved or created. In order to illustrate this powerful tool, we have written three ISPF scripts, which provide three types of information that cannot be obtained through the native RACF interface (see below).

First, for extra user-friendliness, we created a sample ISPF tool with a welcome panel.

Panel:

```
)ATTR DEFAULT(%+à)
       %   TYPE(TEXT)   COLOR(BLUE)
       +   TYPE(TEXT)   COLOR(WHITE)                      SKIP(ON)
       à   TYPE(INPUT)  COLOR(GREEN) CAPS(ON)  JUST(LEFT)
       ú   TYPE(INPUT)  COLOR(GREEN) CAPS(ON)  JUST(LEFT)  PAD(-)
       §   TYPE(OUTPUT) COLOR(BLUE)
       £   TYPE(OUTPUT) COLOR(WHITE) CAPS(OFF) JUST(ASIS)
)BODY EXPAND(¬¬) WINDOW(76,14)
+Command ==>àZCMD
%
%
%    +Search for a Name        %:àcmd1                              +%
%
%    +Search for Last Job Date %:àcmd2        +and User%:àcmd4     +%
%                               (dd.mm.yyyy)
%
%    +Search for TSO Logon Proc%:àcmd3                             +%
%
%+F1=%AIDE +F3=%SORTIE
)INIT
 .HELP = tutorial
 .CURSOR = cmd1
)PROC
 IF (&cmd1 = ' ')
```

```
  IF (&cmd2 = ' ')
   VER(&cmd3,NB)
)end
```

Script:

```
/* rexx */
/* trace all  */
x = msg('off')
ZWINTTL = 'RACF : Sample Request'
call depart
Exit
/*  */
/* parameters */
/*  */
depart:
  Address ispexec
  cmd     = ''
  cmd1    = ''
  cmd2    = ''
  cmd3    = ''
  cmd4    = ''
 'addpop row(6) column(1)'
 'display panel(paselect)'
  rcsave = rc
  If rcsave <> Ø Then call exitko
 'rempop'
  call trt1
return
/*  */
/* process */
/*  */
trt1:
  if cmd1 ¬= ' ' then call nompre cmd1
  if cmd2 ¬= ' ' then call ddo cmd2 cmd4
  if cmd3 ¬= ' ' then call tsolog cmd3
  call depart
exit
/*  */
/* exitko */
/*  */
exitko: procedure
    Parse Arg message
    Address ispexec
   'ADDPOP row(6) column(1)'
    zwinttl = 'RACF : Sample Request'
    If message = '' Then Do
       'control display lock'
       message = 'Processing , please wait ...'
    End
   'display panel(lisreco1)'
   'rempop'
```

```
    Exit
return
```

APPENDIX ONE

The following DB2/REXX procedure can be used to obtain the list of codeusers assigned to a user, and thus a better view of his privileges.

Edit panel: (panompre)

```
)ATTR DEFAULT(£+_)
 £ TYPE(TEXT) INTENS(HIGH)
 + TYPE(TEXT) INTENS(LOW) SKIP(ON)
 ¬ TYPE(INPUT) INTENS(LOW) CAPS(ON) JUST(ASIS)
)BODY EXPAND(//)
+
¬Z+
+      CODEUSER     NAME                              CREATION      DDO
)MODEL
+     ¬Z       +   ¬Z                              +¬Z           +¬Z
)INIT
  .ZVARS = '(TOTO CODEUSER NOM CREATION DDO)'
  .HELP = TUTORIAL
)PROC
)END
```

Script: (nompre)

```
/* REXX */
 PARSE ARG CMD1
 TRACE O
 SUBSYS = 'DB2E'
 /* CONNECT DB2 */
 ADDRESS TSO "SUBCOM DSNREXX"
 IF RC <> Ø THEN S_RC = RXSUBCOM('ADD','DSNREXX','DSNREXX')
 ADDRESS DSNREXX "CONNECT" SUBSYS
 IF RC <> Ø THEN DO
    CALL EXITKO 'CONNECT TO' SUBSYS 'KO' SQLCODE
    ADDRESS DSNREXX "DISCONNECT"
    EXIT
 END
 /* SQL REQUEST */
 SQLCMD = "SELECT"
 SQLCMD = SQLCMD || " USBD_NAME           "
 SQLCMD = SQLCMD || " ,USBD_PROGRAMMER     "
 SQLCMD = SQLCMD || " ,USBD_CREATE_DATE    "
 SQLCMD = SQLCMD || " ,USBD_LASTJOB_DATE   "
SQLCMD = SQLCMD || " FROM"
SQLCMD = SQLCMD || " R5MØØ.USER_BD"
SQLCMD = SQLCMD || " WHERE"
```

```
SQLCMD = SQLCMD || " USBD_PROGRAMMER LIKE '"CMD1"%'"
SQLCMD = SQLCMD || " ORDER BY"
SQLCMD = SQLCMD || " 1 , 2"
/* SQL REQUEST PROCESS */
ADDRESS DSNREXX "EXECSQL DECLARE  C1 CURSOR FOR S1"
ADDRESS DSNREXX "EXECSQL PREPARE  S1 FROM :SQLCMD"
ADDRESS DSNREXX "EXECSQL DESCRIBE S1 INTO :O"
ADDRESS DSNREXX "EXECSQL OPEN C1"
IF RC <> Ø THEN DO
   CALL EXITKO 'OPEN C1 KO' SQLCODE
   ADDRESS DSNREXX "DISCONNECT"
   EXIT
END
I = 1
/* FORMATTED DISPLAY */
ADDRESS ISPEXEC
TABLE = 'REC'||RANDOM(Ø,99999)
 'TBCREATE 'TABLE' KEYS(CODEUSER)
 NAMES(NOM CREATION DDO) NOWRITE'
 IF RC <> Ø THEN CALL EXITKO 'CHECK ON TBCREATE' RC
 DO FOREVER
    ADDRESS DSNREXX "EXECSQL FETCH C1 INTO :CL1,:CL2,:CL3,:CL4 :IV4"
    IF IV4 < Ø THEN CL4 = 'ØØ.ØØ.ØØØØ'
    IF SQLCODE ¬= Ø  THEN LEAVE
    CODEUSER = CL1
    NOM = CL2
    CREATION = CL3
    DDO = CL4
    'TBADD 'TABLE''
    IF RC <> Ø THEN CALL EXITKO 'CHECK ON TBADD' RC
    I = I + 1
 END
 ADDRESS ISPEXEC
 ZWINTTL = 'LIST.RACF - SEARCH FOR NAME'
 'ADDPOP'
 'TBTOP 'TABLE''
 'TBDISPL 'TABLE' PANEL(PANOMPRE) AUTOSEL(NO)'
'REMPOP'
'TBCLOSE 'TABLE''
 IF RC <> Ø THEN CALL EXITKO 'CHECK ON TBCLOSE' RC
ADDRESS DSNREXX "DISCONNECT"
RETURN
/* KO MANAGEMENT */
EXITKO: PROCEDURE
    PARSE ARG MESSAGE SQLCODE
    IF MESSAGE = '' THEN DO
       MESSAGE = 'ERROR :'
    END
    SAY MESSAGE SQLCODE
    EXIT
RETURN
```


APPENDIX TWO

The following ISPF/REXX procedure can be used to obtain the last operation date for a list of user codes, and thus offers a better view of active and inactive user codes

Panels: (paddo)

```
)ATTR DEFAULT(£+_)
 £ TYPE(TEXT) INTENS(HIGH)
 + TYPE(TEXT) INTENS(LOW) SKIP(ON)
 ¬ TYPE(INPUT) INTENS(LOW) CAPS(ON) JUST(ASIS)
)BODY EXPAND(//)
+
¬Z+
+      CODEUSER     NAME                              DDO
)MODEL
+     ¬Z       +   ¬Z                              +¬Z
)INIT
  .ZVARS = '(TOTO CODEUSER NOM DDO)'
  .HELP = TUTORIAL
)PROC
)END
```

Scripts: (ddo)

```
/* REXX */
TRACE O
PARSE ARG CMD2 CMD4
SUBSYS = 'DB2E'
/* CONNECT DB2 */
ADDRESS TSO "SUBCOM DSNREXX"
IF RC <> Ø THEN S_RC = RXSUBCOM('ADD','DSNREXX','DSNREXX')
ADDRESS DSNREXX "CONNECT" SUBSYS
IF RC <> Ø THEN DO
   CALL EXITKO 'CONNECT TO' SUBSYS 'KO' SQLCODE
   ADDRESS DSNREXX "DISCONNECT"
   EXIT
END
/* SQL REQUEST */
SQLCMD = "SELECT"
SQLCMD = SQLCMD || " USBD_NAME           "
SQLCMD = SQLCMD || " ,USBD_PROGRAMMER     "
SQLCMD = SQLCMD || " ,USBD_LASTJOB_DATE   "
SQLCMD = SQLCMD || " FROM"
 SQLCMD = SQLCMD || " R5MØØ.USER_BD"
 SQLCMD = SQLCMD || " WHERE"
 SQLCMD = SQLCMD || " USBD_LASTJOB_DATE = '"CMD2"'"
 SQLCMD = SQLCMD || " AND USBD_NAME LIKE '"CMD4"%'"
 SQLCMD = SQLCMD || " ORDER BY"
 SQLCMD = SQLCMD || " 1 , 2"
```

```
 SAY SQLCMD
 /* SQL REQUEST PROCESS */
 ADDRESS DSNREXX "EXECSQL DECLARE  C1 CURSOR FOR S1"
 ADDRESS DSNREXX "EXECSQL PREPARE  S1 FROM :SQLCMD"
 ADDRESS DSNREXX "EXECSQL DESCRIBE S1 INTO :O"
 ADDRESS DSNREXX "EXECSQL OPEN C1"
 IF RC <> Ø THEN DO
    CALL EXITKO 'OPEN C1 KO' SQLCODE
    ADDRESS DSNREXX "DISCONNECT"
    EXIT
 END
 I = 1
 /* FORMATTED DISPLAY */
 ADDRESS ISPEXEC
TABLE = 'REC'||RANDOM(Ø,99999)
'TBCREATE 'TABLE' KEYS(CODEUSER)
NAMES(NOM DDO) NOWRITE'
IF RC <> Ø THEN CALL EXITKO 'CHECK ON TBCREATE' RC
DO FOREVER
   ADDRESS DSNREXX "EXECSQL FETCH C1 INTO :CL1,:CL2,:CL3 :IV3"
   IF IV3 < Ø THEN CL3 = 'ØØ.ØØ.ØØØØ'
   IF SQLCODE ¬= Ø  THEN LEAVE
   CODEUSER = CL1
   NOM = CL2
   DDO = CL3
   'TBADD 'TABLE''
   IF RC <> Ø THEN CALL EXITKO 'CHECK ON TBADD' RC
   I = I + 1
END
ADDRESS ISPEXEC
ZWINTTL = 'LIST.RACF - SEARCH FOR LAST JOB DATE'
'ADDPOP'
'TBTOP 'TABLE''
'TBDISPL 'TABLE' PANEL(PADDO) AUTOSEL(NO)'
'REMPOP'
'TBCLOSE 'TABLE''
 IF RC <> Ø THEN CALL EXITKO 'CHECK ON TBCLOSE' RC
ADDRESS DSNREXX "DISCONNECT"
RETURN
/* KO MANAGEMENT */
EXITKO: PROCEDURE
    PARSE ARG MESSAGE SQLCODE
    IF MESSAGE = '' THEN DO
       MESSAGE = 'ERROR :'
    END
    SAY MESSAGE SQLCODE
    EXIT
RETURN
```


APPENDIX THREE

The following REXX procedure can be used to obtain a list of users working with a given TSO environment procedure, and so manage typical technical rights.

Panel: (patsolog)

```
)ATTR DEFAULT(£+_)
 £ TYPE(TEXT) INTENS(HIGH)
 + TYPE(TEXT) INTENS(LOW) SKIP(ON)
 ¬ TYPE(INPUT) INTENS(LOW) CAPS(ON) JUST(ASIS)
)BODY EXPAND(//)
+
¬Z+
+      CODEUSER     NAME                              LOGONPROC
)MODEL
+     ¬Z       +   ¬Z                              +¬Z
)INIT
  .ZVARS = '(TOTO CODEUSER NOM TSOPROC)'
  .HELP = TUTORIAL
)PROC
)END
```

Script:

```
/* REXX */
 TRACE O
 PARSE ARG CMD3
 SUBSYS = 'DB2E'
 /* CONNECT DB2 */
 ADDRESS TSO "SUBCOM DSNREXX"
 IF RC <> Ø THEN S_RC = RXSUBCOM('ADD','DSNREXX','DSNREXX')
 ADDRESS DSNREXX "CONNECT" SUBSYS
 IF RC <> Ø THEN DO
    CALL EXITKO 'CONNECT TO' SUBSYS 'KO' SQLCODE
    ADDRESS DSNREXX "DISCONNECT"
    EXIT
 END
 /* SQL REQUEST */
 SQLCMD = "SELECT"
 SQLCMD = SQLCMD || " A.USBD_NAME"
 SQLCMD = SQLCMD || " ,A.USBD_PROGRAMMER"
 SQLCMD = SQLCMD || " ,B.USTSO_LOGON_PROC"
 SQLCMD = SQLCMD || " FROM"
SQLCMD = SQLCMD || " R5MØØ.USER_BD A"
SQLCMD = SQLCMD || " ,R5MØØ.USER_TSO_DATA B"
SQLCMD = SQLCMD || " WHERE"
SQLCMD = SQLCMD || " B.USTSO_LOGON_PROC = '"CMD3"'"
SQLCMD = SQLCMD || " AND B.USTSO_NAME = A.USBD_NAME"
SQLCMD = SQLCMD || " ORDER BY"
```

```
SQLCMD = SQLCMD || " 1 , 2"
/* SQL REQUEST PROCESS */
ADDRESS DSNREXX "EXECSQL DECLARE  C1 CURSOR FOR S1"
ADDRESS DSNREXX "EXECSQL PREPARE  S1 FROM :SQLCMD"
ADDRESS DSNREXX "EXECSQL DESCRIBE S1 INTO :O"
ADDRESS DSNREXX "EXECSQL OPEN C1"
IF RC <> Ø THEN DO
   CALL EXITKO 'OPEN C1 KO' SQLCODE
   ADDRESS DSNREXX "DISCONNECT"
   EXIT
END
I = 1
/* FORMATTED DISPLAY */
ADDRESS ISPEXEC
 TABLE = 'REC'||RANDOM(Ø,99999)
 'TBCREATE 'TABLE' KEYS(CODEUSER)
 NAMES(NOM TSOPROC) NOWRITE'
 IF RC <> Ø THEN CALL EXITKO 'CHECK ON TBCREATE' RC
 DO FOREVER
    ADDRESS DSNREXX "EXECSQL FETCH C1 INTO :CL1 , :CL2 , :CL3"
    IF SQLCODE ¬= Ø  THEN LEAVE
    CODEUSER = CL1
    NOM = CL2
    TSOPROC = CL3
 'TBADD 'TABLE''
 IF RC <> Ø THEN CALL EXITKO 'CHECK ON TBADD' RC
    I = I + 1
 END
 ADDRESS ISPEXEC
 ZWINTTL = 'LIST.RACF - SEARCH FOR LOGON PROCEDURE'
 'ADDPOP'
 'TBTOP 'TABLE''
 'TBDISPL 'TABLE' PANEL(PATSOLOG) AUTOSEL(NO)'
 'REMPOP'
'TBCLOSE 'TABLE''
 IF RC <> Ø THEN CALL EXITKO 'CHECK ON TBCLOSE' RC
ADDRESS DSNREXX "DISCONNECT"
EXIT
/* KO MANAGEMENT */
EXITKO: PROCEDURE
    PARSE ARG MESSAGE SQLCODE
    IF MESSAGE = '' THEN DO
       MESSAGE = 'ERROR :'
    END
    SAY MESSAGE SQLCODE
    EXIT
RETURN
```

Sylvain Danvy and Dominique Cannessant
System Engineers (France)

Installing a Symantec Firewall/VPN 100

In our continuing series on remote security, we again turn our attention to hardware firewalls as a way to protect remote workstations connected to the RACF-protected mainframe. Here we describe the process of installing a Symantec Firewall/VPN 100.

It's hard to believe that just over a year ago I had trouble convincing security expert friends that they needed more than VPN to protect a workstation attached to commercial high-speed Internet. Like any other business, ISPs understand the need to protect their staff's Internet access by hiding them behind a firewall. But few, if any, protect their customers.

Without a firewall between the remote workstation and the Internet, hackers could gain access to the workstation. Once they're there, they simply need to bide their time until a VPN connection is established by the workstation user. It's likely to be an organization's top mainframe support people who first get high-speed Internet at home – so they can answer their 3 am system down phone calls – so it's easy to imagine a hacker having unlimited access to the mainframe simply by waiting for that user to log on to RACF. After all, most support people have few RACF restrictions placed on their IDs.

A year on, most people have a very different view of computer security, hackers, and terrorists, and it's actually been quite difficult to find small hardware firewalls to evaluate for this series of articles. Most of the vendors already in the market have discontinued their present product(s) and hope to have a new product available soon. And it's difficult to keep track of the many others entering the so-called firewall appliance market.

However, one of those vendors is Symantec. Now calling itself an Internet security technology company, Symantec is best known for its (Peter) Norton line of software, especially to anyone who ever supported PC-DOS. On 8 October 2001, a new line of firewalls was announced: Symantec Firewall/VPN 100, 200, and 200R. Symantec already had,

and continues to sell, the Symantec VelociRaptor, a traditional enterprise hardware firewall co-branded with Sun, as well as both firewall and anti-virus software, from the individual desktop to the entire enterprise.

In this article, we look at the Symantec Firewall/VPN 100, intended for between one and fifteen users (twenty at a pinch). It includes one WAN port and four autosense 10/100Mbps LAN ports. The 200 is essentially double the 100, handling up to 30 users, 40 maximum. The 200R adds Symantec Enterprise VPN Client (formerly RaptorMobile) to the 200. The 200 and 200R provide load balancing between their two WAN ports. Ideally, each port is connected along separate paths to different ISPs, such as would be the case using xDSL for one and cable modem technology for the other. None of the three models have licence restrictions on number of users; the numbers quoted are based on performance considerations.

Symantec recommends its VelociRaptor for more than 30 users. It supports Internet connections up to 90Mbps.

OPENING THE BOX

The Symantec Firewall/VPN 100 arrived in a box about one foot square and less than three inches thick. Inside was a metal box about half that size, with one WAN port, four LAN ports, and 17 LED green and yellow status lights on the front, and a nine-pin male serial plug, four DIP switches, a Reset button, and a power rocker switch on the rear. There was also a small outlet where a 6 ft power transformer cord was to be plugged. The transformer plugged directly into the wall with a non-polarized plug: the two blades are equal width, allowing the transformer to be positioned in either of two orientations – extremely useful where the space around a UPS, power bar, or wall power outlet is tight. However, it may still block other outlets unless they are well spread out.

In addition, there were the following:

- 3 ft female to female 9-pin Null Modem serial cable.
- 9.5 ft CAT5 LAN cable.

- Quick Start Card in English, French, German, and Spanish.
- Release notes (including a product contents list).
- CD-ROM.

All of the documentation is common to Models 100, 200, and 200R. The CD-ROM had nothing in the root directory except a folder named English, which in turn had four folders: Adobe, Docs, Readme, and Utilities. Adobe has a Win folder that contained an installation file for Adobe Acrobat Reader. The Utilities folder contained nxtftp.exe and nxtftpw.exe, to be used for firmware updates. Readme contained a .pdf version of the Release Notes. Docs contained a .pdf version of the Quick Start Card and the 120-page *Installation and Configuration Guide*. Since the products had just been released at the time of review, all of the manuals and the CD-ROM were less than two months old.

INSTALLATION

Admittedly each step contains three to five sentences, but there are only four steps on the Quick Start Card. Still, it gets you all the way through physical installation and past the first customization step (Language). You're then directed to the User Interface Help or the CD-ROM's *Installation and Customization Guide*, which in fact provides a much more detailed set of installation steps than the Quick Start Card, including the careful detailing of requirements.

In contrast to the WatchGuard SOHO firewall reviewed in *RACF Update* 25 (August 2001, pp 37-48), the Quick Start Card for the Symantec Firewall/VPN 100 recommends hot plugging:

- The unit is plugged in and powered up before any LAN or WAN cables are connected.
- The WAN cable is plugged into the unit with the broadband modem powered on.
- The (first) LAN cable is plugged in with the PC running.

The value of this approach, if the hardware will handle it, is that the Quick Start Card includes status checking in each step via the LED lights, as well as corrective measures. Unfortunately, one of the best

corrective measures is not stated: read the *Installation and Customization Guide* on CD-ROM. As noted above, it contains much more detailed installation information.

FIRST POWER UP

After power up, several status lights went off and on for about a minute before settling down to just the power indicator and LAN/WAN lights on, displaying green. After connecting the WAN and LAN cables, it again took a while for lights to stabilize. Even after stabilization, the green WAN link LED blinked off briefly every eight seconds. For LAN port 1, where I plugged the LAN cable, the 100 light was green and the <---> light was yellow. The 100 light indicated that the NIC's 100Mbps capability had been correctly autosensed.

Note that Step 3 in the Quick Start Card is confusing (or wrong). It states "If you connect the cable correctly, the LAN/WAN LED illuminates in green." The LAN/WAN LED (diagrammed above the Steps as connected up and down arrows) went green when the unit was powered on, before any cables were connected.

Once the cables are connected, Step 4 instructs that the PC must be rebooted. This is not usually required, as you can start your browser and go to the URL specified: http://192.168.0.1

CUSTOMIZATION

I was then greeted with a one-time choice of languages, with English as the default, and hit the Save button. I immediately saw the Main Set-up page, which is what would appear from now on whenever I entered the above URL. As you might have guessed, this Web site is within the Symantec Firewall.

The Main Set-up page shows the connection status, allows you to choose between the default Obtain IP & DNS Automatically and PPPoE (Point-to-Point Protocol over Ethernet), has a section titled Optional Network Settings where you can specify host name, domain name, and network adapter (MAC) address, and has save, cancel, and refresh buttons at the bottom of the page. A large left sidebar has so

General
- Main Setup
- Static IP & DNS
- Status
- View Log
- LAN IP & DHCP
- Config Password

VPN
- Static Key
- Dynamic Key
- Client Identify

Advanced
- Host IP & Group
- Access Filters
- Special Applications
- Virtual Servers
- Custom Virtual Servers
- Exposed Host (DMZ)
- Advanced PPPoE
- Dynamic DNS
- Routing
- Backup/Analog/ISDN
- Log Settings
- Expert Level

Figure 1: Links to other Web pages

many links to other Web pages (all within the box) that they are categorized (see Figure 1).

CONNECTED TO THE INTERNET

At this point, the Quick Start Card instructions ended, and an inadvertent test – McAfee VirusScan Online automatically checking for updates – indicated that http access to the Internet was working. I checked the *Installation and Configuration Guide*, and found that the Quick Start Card had covered the 'Installation' chapter and the beginning of the 'Configuration' chapter, though a couple of Control Panel and browser settings were not made. These weren't required mainly because the ADSL connection had already been set to use DHCP.

Reviewing the remainder of the 'Configuration' chapter, only the last section, Config Password, was of special interest. It recommends setting a password in an office environment and strongly recommends it if remote configuration is enabled (not the default).

Feeling comfortable that the firewall was doing its job, I plugged my production workstation into the second LAN port, and successfully contacted my ISP's POP3 mail server and viewed a Web page. A tn3270e session to my test mainframe site on the Internet worked perfectly, and an ftp to the same site also worked.

To give the box a fighting chance, especially considering it was such a new product, it only seemed fair to apply any firmware updates that were available. Chapter 10 of the *Installation and Configuration Guide* is entitled 'Firmware Upgrades' and describes the update process. Although there's a detailed, eight-step process to actually do the upgrade, the previous page of text is less than helpful: "These firmware upgrades are available from Symantec's home page."

Symantec is a big company and its home page is full of links to information on its many products. After a lot of false starts, I finally found the Firewall VPN/100 in the tools and downloads section/ Get Product Updates/ enterprise user. The Web page displayed included the following section:

- Solve a technical issue "for help configuring, installing, and troubleshooting your problem with Symantec Firewall/VPN Appliance 100", with four links:
  - KnowledgeBase 2000
  - Releases and updates (none available)
  - Manuals and documentation
  - Contact customer support

Admittedly, if I had read the beginning of the *Installation and Configuration Guide*, entitled 'Service and Support Solutions', the section on 'Technical Support' would have directed me right to http://service.symantec.com where the home/small business user and enterprise user choice was made. The trick, of course, is knowing that the Symantec Firewall/VPN 100 is listed only under enterprise user.

A week later, a firmware update, labelled a hot fix, was available as a .ZIP file in the morning, but, by the afternoon, the entire product family had disappeared from the enterprise user list. This was probably the frequent Webmaster mistake of updating and posting an old copy of a Web page. 10 days later, the product family was back, and there was no 'none' available beside Releases and Updates. However, clicking on the link displayed a Web page stating: "There are no files for Symantec Firewall/VPN Appliance 100".

CONCLUSIONS

The Symantec Firewall/VPN 100 and, by extension, the same design 200 and 200R, are worth serious consideration as hardware firewalls to provide the kind of remote workstation protection from hackers that RACF, and even VPN by itself, cannot offer.

Like the WatchGuard SOHO previously reviewed, they are truly appliances that you can install quickly and walk away from. But that doesn't mean that they can be ignored. Just as viruses are now going from unknown to widespread in less than 24 hours, new hacker techniques may do the same in the future. To stay on top of it all, be sure to keep an eye out for firmware updates and apply them promptly. Both Symantec and WatchGuard provide them, as well as the documentation to install them.

Jon E Pearkins
(Canada)

Comparing firewalls

The Symantec Firewall/VPN 100 (reviewed on pp 47-53) and the WatchGuard SOHO (reviewed in *RACF Update* issue 25 (August 2001)) are both good choices for accessing a RACF-protected mainframe from the small remote office or as a single user at home. So how can you choose between the two? Figures 1 to 5 offer some side-by-side comparisons.

SPECIFICATIONS

Figures 1, 2, 3, and 4 give the facts, figures, and other objective information; a few explanatory notes follow.

	Symantec Firewall/VPN 100	**WatchGuard SOHO**
Maximum users		
(recommended)	15-20	50
(licensed)	Unlimited	10, upgradeable to 25 or 50
Throughput claimed	8Mbps for firewall traffic and 3.6Mbps for 3DES VPN traffic	9Mbps
LAN ports	4 x 10/100Mbps (autosense)	4 x 10Mbps
LAN port status lights	100, 10, <—> (Full duplex)	Link, data
WAN port status lights	Modem (WAN) link	Link, data
Other status lights	Power, Error indicator, LAN/WAN transmit/ receive, back-up active	Mode, on
Power switch	Rocker switch on back	None
VPN	Included	Optional
Autodial back-up	Yes	No
Back-up throughput	230Kbps	Not applicable
Remote management	Yes, but default is off	Yes, but default is off
List price		
(US)	$499	$449
(UK)	£339.57	£315
(Euros)	¤610.09	¤500
(Canadian)	$775	$700
Lowest street price		
(US)	$277.50	$328.09

Figure 1: Comparing the specifications (part one)

Firmware updates	Free for one year, $149 to extend to 3 years, $199 for 3 years of 24/7 service	Free for one year, $95 for each additional year, $150 for 2 years
Size		
(imperial)	11" x 5.5" x 1.25"	6.5" x 6" x 1"
(metric)	280 x 140 x 30 mm	165 x 150 x 25 mm
Weight		
(imperial)	2.3 lb.	10 oz.
(metric)	1.033 kg.	285 g.
Shipping size		
(imperial)	11.75" x 10.25" x 2.75"	10" x 8.5" x 3"
(metric)	300 x 260 x 70 mm	250 x 215 x 75 mm
Shipping weight		
(imperial)	5 lb.	2 lb.
(metric)	2 kg.	1 kg.
Power transformer size		
(imperial)	2.75" x 2.25" x 1.75"	2.25" x 2" x 1.5"
(metric)	70 x 57 x 45 mm	57 x 50 x 38 mm
Polarized power plug?	No	No
Power cord length		
(imperial)	6.2 ft.	6.1 ft.
(metric)	1.89 m.	1.86 m.
Power transformer output	9 volts, 1 amp	12 volts, 0.5 amps
LAN cables included	One 9.5 ft CAT5 (specifications say 6 ft)	One 6.8 ft. CAT5 with non-retractable boots
Processor	ARM ARM7	Toshiba TMPR3907
Processor speed	50MHz	66MHz
Operating system	Proprietary	Proprietary (hardened)
Accelerator	Hifn 7902 built-in encryption chip	Proprietary VPN chip
Flash memory	512KB	1MB
Other memory	4MB RAM	4MB SDRAM
Firewall IP address	192.168.0.1	192.168.111.1
Lowest LAN IP address	192.168.0.2	192.168.111.2
Log format	See Figure 3	See Figure 4
Log display order	Chronological	Reverse chronological

Figure 2: Comparing the specifications (part two)

Notes

Note that the Symantec street price reflects introductory pricing (instant rebate) which expired on 31 December 2001. Lower prices than shown are available for the WatchGuard, but aren't included because:

```
11/20/2001 14:35:57.40 Port Scan attack !!! 195.242.83.223:1728
161.184.154.57:23 Telnet
11/20/2001 16:00:35.55 Port Scan attack !!! 64.12.184.3:80
161.184.154.57:64157 TCP
```

Figure 3: Symantec 100 log

```
              IP   entry duplicated 4 times

2001-11-25-   IP   Packet discarded from 208.179.251.103 port 4942
14:59:28           to 161.184.155.16 port 25 (TCP)(default)
```

Figure 4: WatchGuard SOHO log

- One was NFR (Not For Resale) and required the signing of a WatchGuard distribution agreement.
- Several were auctions on eBay of both new and used units.

The comments on the power transformer are specific to the US/Canadian models that were reviewed. Other countries may have different wall socket configurations.

EVALUATION

The data shown in Figure 5, evaluating the firewalls, is more subjective, and is based on tests of each firewall. Explanations of each follow.

Evaluation explanations

Note that:

- 'Firewall-to-Web site integration' looks at how easy it is (or is not) to move between the Web pages hosted inside the firewall itself, and those pages hosted by the vendor on its Web site.
- A product labelled as 'Seamless' means only that you can't tell, without looking at the Address field in the Web browser, whether you're on the firewall or the vendor's Web site. It doesn't imply that the firewall's Web pages include all the links to the vendor's Web site that you would want or need.

	Symantec Firewall/ VPN 100	WatchGuard SOHO
Firewall to Web site integration	An icon to Symantec home page	Seamless
ShieldsUp	"Invulnerable to outside discovery, connection and attack"	"Invulnerable to outside discovery, connection and attack"
Leaktest	Failed	Failed
ftp Download test	No measurable slowdown	No measurable slowdown
ftp Upload test	No measurable slowdown	No measurable slowdown
dslreports.com	"Healthy Set-up"	"Healthy Set-up"
hackerwhacker.com	0 of 1711 IP ports open, no NetBIOS information available	0 of 1711 IP ports open, no NetBIOS information available
Hibernation recovery	Too slow	OK

Figure 5: Evaluating the firewalls

- ShieldsUp and Leaktest are popular firewall tests hosted on Steve Gibson's grc.com site:
  - ShieldsUp checks your Internet connection for common hacker entrances, including visible services that attract the attention of automated hacker tools that spend their lives cruising the Internet.
  - Leaktest is more controversial. It looks at what a rogue program that has found its way on to your workstation might do to communicate to its owner (a hacker). Steve believes that firewalls should also protect your privacy, not just your security. Others point out that you should have the anti-virus software and e-mail security patches in place to prevent the malicious program from getting on your workstation in the first place.
- The ftp tests used a 4.11MB (4,314,156 bytes) file named TEST.ZIP, which is really a renamed copy of 57BTFVDR.ZIP from C:\WINNT\java\Packages in Windows 2000 Professional. The file was uploaded and downloaded to the ISP's Web space using the command level ftp client on Windows 2000. The ADSL line was throttled (by the ISP) to 2.5Mbps download and 1Mbps upload.

- The actual figures weren't included in the table because they all differed less than differences in the same test without a firewall. For the record, here they are:
  - Symantec upload 41.62 sec.
  - Symantec download 17.21 sec.
  - WatchGuard upload 41.61 sec.
  - WatchGuard download 15.77 sec.
  - No firewall upload 41.61 sec.
  - No firewall download 20.62 sec. (average).

  The final test was performed six times with the following values: 19.83, 22.94, 20.30, 19.37, 21.19 and 20.11 seconds.
- The dslreports.com testing was its Shield Probe test done at:

  http://www.dslreports.com/scan
- The hackerwhacker.com testing was a set of tests, mainly a scan of 1711 ports and NetBIOS visibility, that requires a free sign-up and then can be done only once. Push the Scan button on the home page.
- Hibernation recovery refers to how quickly the connections are re-established when a workstation is awakened from Hibernation. Hibernation is a rapid shut-down and start-up capability that allows complete powering down of the workstation, and complete recovery of the state of the machine at shut down. It was first introduced in Windows 2000.
- The test was performed on Windows 2000 Professional, with Office XP. Outlook 2002 was set to scan for mail every minute. Both the firewall and the ADSL modem were left powered up during Hibernation. To pass the test, the firewall had to re-establish the workstation's Internet connection fast enough to avoid a Send/Receive Error in Outlook.

Jon E Pearkins
(Canada)

Information point – reviews

ARIZONA STATE UNIVERSITY – http://www.asu.edu/it/fyi/mvs/racf

Arizona State University (ASU) does a very nice job of documenting the use of RACF, including a lot more than even a departmental security administrator would normally need to know. The Web pages have a clean look, and the information is divided up as follows:

- General information regarding RACF.
- Log-on passwords.
- JCL for batch jobs submitted to MVS from other systems.
- How to use ISPF option 9.R to communicate with RACF.
- How to use the utility batch program to communicate with RACF.
- How access to disk files is controlled.
- How access to tape volumes is controlled.
- Common RACF commands
  - ADDSD
  - ALTDSD
  - ALTUSER
  - DELDSD
  - LISTDSD
  - LISTUSER
  - PASSWORD
  - PERMIT
  - RALTER

– RLIST

– SEARCH.

Although not show above, each command is also described, to help the user determine, or remember, the right command for the task at hand. But, as you can see, there's one thing that prevents its use in other installations: ASU's local ISPF fast path of =9.R for RACF. Out of the box from IBM, it is =M.3, but many installations have made their own changes.

Looking a little deeper, you may find other local differences. For example, in Log-on passwords, you'll find that they expire after 90 days at ASU. I've worked on systems where password expiry is set to anywhere between 30 days and six months (even Never on occasion). And, of course, ASU has its own name for its different computer systems, as well as the areas that perform specific functions, such as the Computer Accounts Office.

1987 RACF Help Files

The RACF Commands are documented by creating Web pages from the TSO HELP output for each command. But not the current ones – the ones from 1987!

Initially, this sounds bad, but a quick look at a recent (OS/390 2.6) version of the help files reveals why. The 1987 LISTDSD help is 157 lines long, which takes less than 7 scrolls to go through on a typical Web browser running full screen at 800x600 resolution. In OS/390 2.6, it is 692 lines and doesn't include the list of error messages that 1987 did. Take a more complex command, ALTUSER, and today's Help has grown to 3,182 lines (still without the list of error messages).

On the other hand, using 1987 Help files misses the large number of changes to RACF that have occurred since then. Most glaring is Unix support, for z/OS Unix System Services (USS). Clearly, ASU doesn't use Unix on its mainframe, so, if your organization does, this site will be a lot less useful than it will for others.

ASURITE – http://www.asu.edu/it/fyi/accounts

ASU has clearly gone to a lot of effort to effectively administer student, faculty, and staff usage of computing resources. A university is like a corporation where over 90% of users (students) have the following characteristics:

- No one stays more than four years.
- Most people share their time among five jobs.
- Everyone changes jobs every four months.
- Everyone gets four months vacation every summer.

Even telemarketing companies aren't that bad. If high turnover is the issue, universities might have some experience that can be helpful. ASU is especially interesting because it doesn't just handle students, who only have minimal access, but also the power users and support personnel you would expect to find among the ranks of faculty and staff.

Everyone at ASU who needs to use the academic and administrative computing facilities, no matter what platforms, must have an ASURITE account, with its single user ID and password. ASURITE is the ASU Rational Information Technology Environment. In the left sidebar, you'll see, amongst other things, 'What is ASURITE?'

http://www.asu.edu/it/fyi/asurite

There you'll find links within the text of the page. One is to appropriate policies and guidelines, which takes two clicks to get you to the very detailed 'ASU Computer, Internet and Electronic Communications Policy', which is part of the *Academic Affairs Policies and Procedures Manual*:

http://www.asu.edu/aad/manuals/acd/acd125.html

A second link is near the bottom: unannotated specification in PDF. There you'll find the latest revision, currently 22 pages (80KB) from October 1996, describing ASURITE in full:

http://www.asu.edu/it/fyi/asurite/fulldoc/asurite.pdf

UNIVERSITY OF OKLAHOMA (OU) – http://www.ou.edu/dcts/training/tips/racf.htm

The University of Oklahoma site complements ASU's RACF site. Although very complete in other ways, ASU only describes the use of PF keys on the menu-driven, fill-in-the-blanks ISPF panels for RACF. OU shows some of the common RACF ISPF panels and describes how to use them, and includes possible values for major fields.

Note that, although it's only a single long Web page, there's quite a bit of installation-specific information, such as time limits, phone numbers, and position titles.

THE RACF PASSWORD CRACKER PAGE

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

We've talked about the OS/390-MVS Cyber Mall in previous articles, and Thierry Falissard is a familiar name to *RACF Update* readers, but the RACF Password Cracker page deserves special mention. First, however, be warned: it's dominated by a discussion that parallels that held a decade earlier on ethical hacking – is it dangerous to make RACF password cracking programs generally available? The language in the excerpts from discussion forums may offend some.

Thierry's page is kept relatively up-to-date with a comprehensive set of information and links, including some to password cracker programs, that can help you more accurately determine the level of security you currently have with RACF passwords in your environment. And what to do about it if you don't like what you find.

Even if you've read Thierry's article in *RACF Update* issue 22 ('The fuss about passwords and password crackers', November 2000), his cracker Web page is still worth looking at as it contains a lot of additional and updated information.

SANS – http://www.sans.org/infosecFAQ/authentic/authentic_list.htm

SANS (System Administration, Networking and Security) Institute has also been mentioned in previous articles. The Authentication section of

the Reading Room has several articles on passwords and password cracking. But there's also a detailed introduction to RACF from March 2001 at:

http://www.sans.org/infosecFAQ/authentic/RACF.htm

An Introduction to Security Features in Security Server (RACF) by Jeromy R Denton was written to help those familiar with security but not familiar with RACF, especially those who find themselves assigned to secure or audit a RACF system. In addition, the 'References' section at the end of the article lists three AuditNet articles on RACF security reviews and audit programs. One word of caution, however: the date beside each article in the 'References' appears to be the date Mr Denton found them, rather than the date they were written.

Jon E Pearkins
(Canada)

Call for papers – share your expertise and earn money at the same time!

Why not share your expertise and earn money at the same time? *RACF Update* is looking for technical articles on mainframe security issues and developments and sample code that experienced RACF practitioners have written to make their life, or the lives of their users, easier.

Articles can be of any length and can be sent or e-mailed to Fiona Hewitt at any of the addresses shown on page 2.

More information about contributing an article to a Xephon Update, and an explanation of the terms and conditions under which we publish articles, can be obtained from our Web site, at www.xephon.com/nfc

ASPG's Easy RACF Query (ERQ) Version 2.0 includes an on-line function to allow for automated security administration, simplifying the production of reports, generation of RACF commands, and streamlining of clean-up tasks. Help messages guide the user through the product.

A custom-reporting API-type interface retrieves RACF information for REXX and CLIST custom-written RACF applications. Users have access to both the live and archived RACF database for writing in-house, custom applications.

URL: http://www.aspg.com
URL: http://www.software-europe.co.uk

* * *

Vanguard Security Solutions Version 4 includes Vanguard Enforcer, ezRESET, Administrator, Advisor, and Analyzer. Vanguard Identity Manager, formerly Password Administrator, has been integrated with ezRESET for RACF via a new user interface. The new ezRESET Detail Report lists RACF user ID activity, while the APF Libraries Summary and Detail Report helps monitor APF library usage.

A new active alert in the Real Time Notification feature of Advisor notifies the system administrator whenever a specific RACF user ID is activated.

URL: http://www.go2vanguard.com

* * *

Eberhard Klemens' ETF/R Release 1.2 eliminates the need for an IPL after CLASS or ROUTER TABLE changes. It also allows dynamic refreshes of installation RACF exits without an IPL.

ETF/R, also known as the EKC Firecall Tool for RACF, allows on-demand controlled usage of special high-access capabilities during an emergency situation.

URL: http://www.ekcinc.com
URL: http://www.software-europe.co.uk

* * *

Consul/eAudit (CeA) Version 3.1 adds OS/400, SAP R/3, Compaq (Tandem) SafeGuard, and Novell 4/5 to its existing list of platforms: z/OS with RACF, AIX, Windows NT/2000, HP-UX, Sun Solaris, Lotus Notes, eTrust Access Control for NT and Unix, Microsoft Internet Information Server (IIS), Cisco routers and Pix firewall, and CheckPoint FireWall-1.

CeA monitors all network activity, consolidates the data into a central database, audits the data against active security policies, and provides periodic exception reporting; severe SNMP messages from firewalls are delivered immediately as alerts. Web browser access is also provided to the database.

URL: http://www.consul.com

* * *