IBM Systems Group

I1: z/OS Security Server Update

Vanguard Enterprise Security Expo
May, 2005

Walt Farrell, CISSP
z/OS Security Design
IBM Poughkeepsie
wfarrell@us.ibm.com

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

DB2*
e-business logo
IBM*
IBM eServer
IBM logo*
OS/390*
RACF*
z/OS*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

UNIX is a registered trademark of The Open Group in the United States and other countries.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- **z/OS Version 1 Release 5**
  - Dynamic RACF Templates
  - Multilevel Security
  - RACF Support for DB2 Version 8
  - PKI Services
  - Packaging

Agenda

- **z/OS Version 1 Release 6**
  - Common Criteria
  - Dynamic Class Descriptor Table (CDT)
  - Password Enveloping and LDAP Change Log Support
  - Multilevel Security Auditing

Agenda

Planned for z/OS Version 1 Release 7

- RACF USER-related enhancements:
  - Mixed-case passwords
  - Detect or Prevent password recycling
  - Maintain revoke date when resuming users
  - Improve SETR INACTIVE processing for new users
- RACF Availability enhancement:
  - Automatic RVARY SWITCH to backup for some errors
- RACF API enhancement:
  - R_admin functions to extract USER, GROUP, and CONNECT information
- RACF Security enhancement for servers:
  - Nested ACEEs
- Several PKI Services enhancements

z/OS Security Server (RACF) Update: V1R5

RACF Dynamic Templates

What are the “RACF Templates”?

- **Map how profiles are written on the RACF database.**
- **Are updated to add new segments or fields for line items, either at a release boundary or in a PTF.**
- **Exist in three places:**
  - The latest version shipped with RACF
  - The version on the database, written there by utility IRRMIN00
    - PARM=NEW   initialize new database
    - PARM=UPDATE   update the templates on existing database
  - The in-storage version
    - Built by RACF Initialization and used when accessing profiles
    - Can only be updated via IPL

Issues with the RACF Templates

- **Install a new release of z/OS. If IRRMIN00 not run**
  - RE-IPL required
- **IRRMIN00 requires correct IRRTEMP1 source. Latest level not obvious.**
    - $/VERSION HRF7707
    - $/VERSION OA01234
  - If wrong level used RE-IPL required
- **Apply a PTF with template changes**
  - RE-IPL required even if no modules in PTF require IPL
- **Could mistakenly run IRRMIN00 to initialize the database rather than update it, wiping out database.**

Many consider these issues to be system outages

What are "*Dynamic* RACF Templates"

- **RACF Initialization builds the in-storage templates automatically from the latest level whether or not IRRMIN00 PARM=UPDATE was run**

- **IRRMIN00 PARM=NEW and PARM=UPDATE automatically writes the latest level of templates to the database**

- **IRRMIN00 PARM=UPDATE will not write down-level templates to a database.**

- **New templates can be activated by a new option on IRRMIN00, PARM=ACTIVATE**

- **IRRMIN PARM=NEW no longer works against a RACF data set which is currently used by RACF on current system.**

Dynamic RACF Templates…

- **Are no longer shipped in source format as IRRTEMP1! They are shipped as a module in compiled format as IRRTEMP2.**
- **Contain the release and apar level so RACF can determine the latest level of the templates:**

  $/VERSION FMID/APAR# rrrrrrrr.aaaaaaaa

```
$/VERSION HRF7708 00000010.00000000
$/VERSION OA01234 00000010.00000010
$/VERSION OA01567 00000010.00000020
$/VERSION HRFxxxx 00000023.00000020
```

- **SET LIST operator command displays the in-storage template level and the dynamic parse level in effect on the system.**

```
RACF STATUS INFORMATION:
    TEMPLATE VERSION             - HRF7708 00000010.00000000
    DYNAMIC PARSE VERSION        - HRF7708
```

Dynamic RACF Templates…

- **During IPL, RACF Initialization puts the templates in storage**

- **If the Master Primary database level is higher or the same as IRRTEMP2, RACF builds them from the database**

- **Otherwise, RACF builds the in-storage templates from IRRTEMP2 and issues message:**

```
ICH579E RACF TEMPLATES ON DATABASE ARE DOWNLEVEL:
    HRF7708 00000000.00000000; USING TEMPLATES AT LEVEL
    HRF7708 00000010.00000000 FROM IRRTEMP2.
    RUN IRRMIN00 PARM=UPDATE
```

IRRMIN00

- **No longer makes use of the SYSTEMP data set, which customers typically pointed to SYS1.MODGEN(IRRTEMP1). Now it gets the templates from IRRTEMP2.**

- **Fail PARM=NEW if the output database is active on the system where IRRMIN00 is invoked.**

- **Will not apply downlevel templates to a database.**

- **Makes templates active dynamically for the new PARM=ACTIVATE invocation when the templates on the active master primary database are a higher level than the in-storage templates.**

IRRMIN00…

- **PARM=NEW**
  - Formats a non-VSAM DASD data set as a RACF database.
  - Now fails if invoked against an active database on the system where IRRMIN00 is invoked
- **PARM=UPDATE**
  - Writes new templates to the database
  - Now fails if new templates are not at higher level than ones in database
- **PARM=ACTIVATE**
  - If the active master primary database has higher level templates than those in storage, they are copied to storage

z/OS Security Server (RACF) Update: V1R5

Multilevel Security

Multilevel Security

- **Multilevel security is the ability to mix different categories and classes of information within the same computing environment in a controlled manner**
- **Evolved from level and categories, through SECLABELs (RACF 1.9)**
- **With z/OS V1.5 multilevel security is extended to:**
  - UNIX System Services
    - files and directories
    - processes
    - sockets
  - Rows within a DB2 table
  - TCP/IP networks
- **Additional Information in these sessions:**
  - I10: Multilevel Security (MLS) Update (Wed, 11:00)

z/OS Security Server (RACF) Update: V1R5

RACF Support for DB2 Version 8

RACF Support for DB2 Version 8

- **Ever since OS/390 R4, RACF has provided a "plug-in" DB2 External Security Module (DSNX@XAC) for DB2**
  - Shipped with RACF in 'SYS1.SAMPLIB(IRR@XACS)
- **Starting with DB2 Version 8 (GA: March 2004), this plug-in is now shipped with DB2 in the SDSNSAMP library, member DSNXRXAC**
  - FMID: HDRE810
- **Support for the new DB2 SEQUENCE object**
  - Two new RACF general resource classes: MDSNSQ, GDSNSQ
- **Support for long DB2 names**
- **ACEE available to DSNX@XAC in many cases where it was not before**
  - **"-" commands from TSO or the MVS console**

RACF Support for DB2 Version 8…

- **Multilevel Support:**
  - DB2 Version 8 allows the assignment of SECLABELs to rows within a table
  - Several existing DB2 RACF general resource classes updated with SLBLREQ=YES to require a SECLABEL if SETR MLACTIVE is in effect
- **Note: Use of RACF “plug-in” exit is not required for row-level multilevel support**

z/OS Security Server (RACF) Update: V1R5

PKI Services

PKI Services Overview

- **PKI Services is a z/OS component which provides a complete certificate authority**
- **Full certificate lifecycle management**
  - User requests driven by customizable web pages
  - Automatic or administrator approval process
  - End user or administrator revocation process
- New news: PKI Services for z/OS V1R5 now certified as Identrus-compliant for CA software
  - Rich Guski will discuss this further on Thursday, in session H13 at 9:15

PKI Services Enhancements with z/OS V1R5

- **Certificate Revocation Lists (CRLs)**
  - The distinguished name of the CRL can now be placed in certificates
  - CRLs can be partitioned within the LDAP name space
  - …. simplifies searching of CRLs
- **Performance Improvements**
  - New VSAM indices (status and requestor)
  - Use of system SSL services

PKI Services Enhancements with z/OS V1R5

Certificate Suspension

- Prior to z/OS V1.5, certificates could be either ‘active’, ‘pending approval’, ‘revoked’, or expired.

- With z/OS V1.5, certificates may be suspended for a period of time.
  - Suspended certificates appear on the next CRL with a reason code of certificateHold
  - New certificate status of ‘SUSPENDED’
  - MaxSuspendDuration
    - New CertPolicy keyword to indicate length of the suspended grace period in days or weeks

z/OS Security Server (RACF) Update: V1R5

Packaging

z/OS V1R5 Packaging

- **The z/OS V1.4 Security Server contains:**
  - RACF, DCE Security Server, Firewall Technologies , LDAP Server, Open Cryptographic Enhanced Plug-in (OCEP), Network Authentication Services, PKI Services
- **With z/OS V1.5, the Security Server contains:**
  - RACF
- **The new z/OS V1.5 Integrated Security Services element contains:**
  - DCE Security Server, Firewall Technologies , LDAP Server, Open Cryptographic Enhanced Plug-in (OCEP), Network Authentication Services
- **PKI Services is moved to the z/OS V1.5 Cryptographic Services element**

z/OS Security Server (RACF) Update

z/OS V1R6

z/OS Security Server (RACF) Update: V1R6

Common Criteria

Common Criteria

- **Common Criteria certification for z/OS R6 completed:**
  - **Labeled Security Protection Profile (LSPP) at Evaluation Assurance Level 3+ (EAL3+)**
  - **Controlled Access Protection Profile (CAPP) at EAL3+**

- **See:**
  - http://www.ibm.com/servers/eserver/zseries/security/ccs_certification.html
  - http://www.bsi.bund.de/zertifiz/zert/reporte.htm#Grossrechner_Systeme

z/OS Security Server (RACF) Update: V1R6

Dynamic Class Descriptor Table (CDT)

Why *Dynamic* CDT?

- **To update the RACF Class Descriptor Table and Router Table the installation must:**
  - Write assembler code
  - Assemble and LinkEdit modules
  - IPL the system
    - Creates availability problem if running 24x7 production environment
- **Many customer requirements have requested the ability to update the RACF CDT with no IPL**
- **Solution in z/OS V1R6**:
  - Dynamic Class Descriptor Table
  - Router Table must be updated only for exceptions

Customer Value of Dynamic CDT Support

- **Availability**
  - No IPL necessary to add, update, or delete an installation-defined class
- **Ease of Use**
  - RACF commands can be used to add an installation-defined class
    - No ASSEMBLER coding required
    - No update to RACF Router Table required when adding an installation-defined class
    - Easier to change attributes of a class

Easy !!!

Summary of steps to Create a Dynamic Class

- **Use new IBM class named CDT to create a class definition**

- **Use new segment CDTINFO to define class attributes**
  - Use the RDEFINE and RALTER commands to define the class attributes – profile in the CDT class
    - RDEFINE CDT dynamic-class-name UACC(NONE) CDTINFO(class-attribute-1 class-attribute-2 ...)

- **Use the SETROPTS command to build the Dynamic CDT in the Dataspace**
  - SETROPTS CLASSACT(CDT) RACLIST(CDT)

Related Enhancements in RACF

- **RACF Router Table**
  - Updates are no longer required for new classes or new REQSTOR/SUBSYS combinations

- **RACROUTE REQUEST=STAT**
  - New keyword allows sequential search of classes in CDT

- **SETROPTS LIST Enhancement**
  - Class names alphabetized

- **Class Name Restrictions Relaxed**
  - Minimum length of class name is 1 character (was 4 characters)
  - Dynamic classes can have a number as the first character

z/OS Security Server (RACF) Update: V1R6

Password Enveloping and LDAP Change Log

What is Password Enveloping / LDAP Change Log?

- **Challenge**
  - **Currently, RACF can receive password updates, but can not send local changes outbound (without exits)**
- **Solution**
  - **Allow outbound-password update propagation**
  - **Designed for use by IBM Directory Integrator (IDI) 5.1.2**
  - **Available z/OS Releases 3, 4, and 5 via APAR:**
    - OA03853 – RACF updates
    - OA03854 – SAF updates
    - OA03857 – LDAP updates

What is Password Enveloping? …

- **Three parts to the solution:**

1. **RACF**
   - Mechanisms for storage and retrieval of changed user definitions (including passwords).
2. **LDAP**
   - Change log support for SDBM (RACF) back end.
   - LDAP interface to retrieve enveloped changed user/password information.
3. **IBM Directory Integrator (IDI)**
   - Event handler for polling z/OS LDAP change log.
   - Java method for decrypting the RACF password envelope.
   - Sample assembly line which detects a RACF password change, retrieves the password envelope, decrypts it, and applies the password to an entry in IBM Directory Server.

z/OS Security Server (RACF) Update

Enhanced SECLABEL Auditing

z/OS V1R6 Multilevel Security Audit Enhancements

- **Multilevel Security Auditing (SECLABELAUDIT) enhancements**
  - Extends the auditing function of RACF
  - Meets requirements for evaluation of z/OS V1R6 to the Common Criteria for certification to the
    - Labeled Security Protection Profile (LSPP) at Evaluated Assurance Level (EAL) 3+.
    - Controlled Access Protection Profile (CAPP) at Evaluated Assurance Level (EAL) 3+.

z/OS V1R6 Multilevel Security Audit Enhancements

- **What is SECLABELAUDIT**

  - Provides additional auditing of access attempts to protected resources based on the auditing option in the profile of the security label associated with the resource

  - Enabled/Disabled by:
    - Activating/Deactivating the SECLABEL class
    - Enabling/Disabling the SETROPTS SECLABELAUDIT option SETR SECLABELAUDIT/NOSECLABELAUDIT

z/OS V1R6 Multilevel Security Audit Enhancements

❑ Overview of Multilevel Security Auditing

- Auditing based on SETROPTS SECLABELAUDIT has been changed such that:
  - Auditing is also done based on the security label of the user if it is different than the resource's security label and the resource's security label did not request auditing.
- This support has been extended to existing RACF Services as well as z/OS Unix System Services (callable services)
- Enabled/Disabled by:
  - Activating/Deactivating the SECLABEL class
  - Activating/Deactivating the existing SETROPTS option - SECLABELAUDIT/NOSECLABELAUDIT

z/OS Security Server (RACF) Update

z/OS V1R7 Planned Items

RACF USER-related Enhancements:
Mixed-Case Passwords

- Allows RACF to distinguish between upper- and lower-case characters in passwords.

- Supported by TSO/E, CICS TS 3.1 (and 2.2 and 2.3 via PTF), Console logon, JOB statements, and z/OS UNIX functions.

- Controlled by SETR PASSWORD(MIXEDCASE | NOMIXEDCASE)
  - Do not enable mixed-case passwords unless all local systems sharing RACF DB are at z/OS R7
  - For RRSF, RACF will ensure passwords are in upper-case if sent to an RRSF node at z/OS R6 or earlier.

RACF USER-related Enhancements: Mixed-Case Passwords…

- Additional SETROPTS password rules:
  - NATIONAL
    - *# (X'7B'), $ (X'5B'), and @ (X'7C')*
  - MIXEDCONSONANT
    - Upper- or lower-case consonants (A-Z, a-z)
  - MIXEDVOWEL
    - Upper- or lower-case vowels (a, e, i, o, u, A, E, I, O, U)
  - MIXEDNUM
    - Upper- or lower-case alphabetic, or numeric, or national
    - At least one upper-case alpha or national, one lower-case alpha, and one numeric
- Old rules (ALPHA, ALPHANUM, CONSONANT, VOWEL, NOVOWEL) will **not** match lower-case alphabetic characters.

RACF USER-related Enhancements: Mixed-Case Passwords…

- Example of password rules:
  - SETROPTS PASSWORD
    - RULE1(LENGTH(8) ALPHANUM(1:8))
      - Accepts passwords of length exactly 8, containing only upper-case alphabetic or national or numeric, with at least one alphabetic or national and at least one numeric
    - RULE2(LENGTH(6:8) MIXEDNUM(1:8))
      - Accepts passwords of length 6 through 8, containing mixed-case alphabetic or national or numeric, with at least one upper-case alphabetic or national, one lower case alphabetic, and one numeric.
    - RULE3(LENGTH(5:8) NATIONAL(3) MIXEDNUM(1:2,4:8)
      - Like RULE2, except requires a national character in position 3 and will allow passwords of length 5 through 8.

RACF USER-related Enhancements: Mixed-Case Passwords…

- Notes:
  - RACF will remember whether a user has ever had a mixed-case password. If not, when comparing a password entered by the user RACF will check both the value as presented to RACF and the upper-case version of that value.
  - When the user is changing his password, RACF will check that the new password and current password, when converted to upper-case, are different. Example:
    - If current password is ABCD
    - Then new password aBcD will be rejected

RACF USER-related Enhancements: Detect or Prevent Password Recycling

- Problem: Users can change passwords repeatedly and recycle their password history, keeping same password.

- Part 1 of Solution: With SETROPTS AUDIT(USER) in effect, RACROUTE REQUEST=VERIFY (logon, etc.) processing will create a type 80 SMF record indicating a password change.

RACF USER-related Enhancements: Detect or Prevent Password Recycling…

- Part 2 of Solution: SETROPTS PASSWORD(MINCHANGE(nnn))

- The MINCHANGE value specifies the minimum lifetime of a user’s password, from 0 (not limited) up to the SETR PASSWORD(INTERVAL(mmm)) value.
  - Before nnn days, a user cannot change his/her own password again.
  - Helpdesk personnel authorized via IRR.PASSWORD.RESET need CONTROL authority to change a user’s password before nnn days.
  - SPECIAL and group-SPECIAL users can change another user’s password during that interval, but not their own password.

RACF USER-related Enhancements: Maintain revoke date when resuming users

- Problem: Administrator specifies
  ALTUSER U1 REVOKE(mm/dd/yy)
  then U1 forgets password, becomes revoked early, and administrator resumes U1.

  RACF removes the REVOKE date.

- Solution: RACF will keep the revoke date.

- ALTUSER has new keywords NOREVOKE, NORESUME which will clear the REVOKE or RESUME dates, if present.

- LISTUSER and LISTGRP will show REVOKE and RESUME dates, even if in the past.

RACF USER-related Enhancements: Improve SETR INACTIVE processing for new users

- Problem: SETR INACTIVE(30) specified. Administrator   creates new user U1, who does not logon for 45 days.

  When U1 does logon, RACF does not consider him inactive, and allows the logon.

- Solution: RACF will put the user's creation date into the LJDATE field during ADDUSER processing. Then RACROUTE REQUEST=VERIFY (logon, etc.) processing will have a value to use for checking inactivity.

- LJTIME is not set during ADDUSER, so logon processing and LISTUSER and applications can still tell the user has never signed on.

RACF Availability Enhancement: Automatic RVARY SWITCH to backup for some errors

- Problem: RVARY SWITCH is needed to recover from device errors on primary RACF DB, but
  - It can take awhile to issue this command, especially if operator needs to supply the password.
  - RVARY cannot work while requests to use the DB are in process, so even after entering password, operator must VARY the device offline.

- Improvement:
  - If major device errors have occurred, affecting RACF and other users of the device, operator can VARY the RACF primary DB device offline (V nnn,OFFLINE,FORCE).
  - z/OS will terminate any outstanding requests with I/O error.
  - RACF will detect this I/O error, see device is offline, and automatically RVARY SWITCH to the backup
    - No password needed
    - SWITCH will happen on all systems in SYSPLEX Communication.

RACF Availability Enhancement: Automatic RVARY SWITCH to backup for some errors…

- Notes:
  - RVARY is still the preferred method for many cases.
    - VARY will affect all applications using data on that volume
  - However, if the device is really broken, the other applications are probably in trouble, anyway.

RACF API Enhancement: R_admin extract function for USER, GROUP, and CONNECT info

- Problem: R_admin callable service allows programs to issue RACF commands, including LISTUSER and LISTGROUP, but:
  - 1. Output of commands is not a programming interface
  - 2. Output is difficult to parse to extract the needed data
  - 3. RACF restricts output to 4096 lines
- Solution: New R_admin functions to extract USER, GROUP, or CONNECT info

RACF API Enhancement: R_admin extract function for USER, GROUP, and CONNECT info…

- New USER-related functions:
  - Extract USER
  - Extract next USER
  - Extract CONNECT
- New GROUP-related functions:
  - Extract GROUP
  - Extract next GROUP
- Data returned in a structured format
  - Segment name
  - Field name
  - Data

RACF API Enhancement: R_admin extract function for USER, GROUP, and CONNECT info…

- Problem state callers require access to FACILITY resource:
  - IRR.RADMIN.LISTUSER for USER-related extract functions
  - IRR.RADMIN.LISTGRP for GROUP-related extract functions
- Normal LISTUSER and LISTGRP security rules also apply

RACF Security Enhancement for Servers: Nested ACEEs

- Scenario: A server authenticates a client, creates ACEE, and then does access checking.

- Problem: Sometimes a check should use the server identity, not the client identity.
  - Example: Server may use SSL or TLS for communication security, but after client authentication occurs, it may be the client (today) who needs authority to use ICSF crypto services or keys.

- This is solved for FTP today, in different ways depending on z/OS release, via PTFs

- Not solved for other servers, though, and a fix like the one in FTP is very complex

  - We need a simpler solution

RACF Security Enhancement for Servers: Nested ACEEs

- Solution:
  - The server tells RACF to create a client ACEE, but to also embed a copy of the server ACEE in the client ACEE, as an ENVR object
  - The administrator (only if instructed by server documentation) tells RACF to use the embedded ACEE.
    - Example: RALTER CSFSERV CSFENC
      APPLDATA('RACF-DELEGATED')
  - Server then uses RACROUTE REQUEST=FASTAUTH to do the authorization check
  - FASTAUTH first checks client authority to the resource, and if that fails, checks server authority

PKI Services Enhancements

- Support for DSA (Digital Signature Algorithm) in key generation and signing
  - Today only RSA supported
- Enhancement to CRL Distribution Point information: Support URI to indicate location of Certificate Revocation List
  - Today only the DN (distinguished name) format supported
- Create ARL (certificate revocation list) for CA certificates generated by PKI services
  - Today PKI Services creates CRL only for user certificates
- Provide basic OCSP (Online Certificate Status Protocol) responder support
  - Today OCSP support, if desired, requires 3rd party provider

Summary

- **z/OS Version 1 Release 5**
  - Dynamic RACF Templates
  - Multilevel Security
  - RACF Support for DB2 Version 8
  - PKI Services
  - Packaging
- **z/OS Version 1 Release 6**
  - Common Criteria
  - Dynamic CDT
  - Password Enveloping and LDAP Change Log Support
  - MLS Auditing

Summary

- **z/OS Version 1 Release 7**
  - USER-related:
    - Mixed-case passwords
    - Detect or Prevent password recycling
    - Maintain revoke date when resuming users
    - Improve SETR INACTIVE processing for new users
  - Availability:
    - Automatic RVARY SWITCH to backup for some errors
  - Programming:
    - R_admin functions to extract USER, GROUP, and CONNECT information
  - Server Security:
    - Nested ACEEs
  - PKI Services Enhancements