IBM TRAINING

Session S17

z/OS Security Update

Walt Farrell, CISSP, z/OS Security Design, IBM

IBM
SYSTEM z9 AND zSERIES EXPO
October 9 - 13, 2006

Orlando, FL

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.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* 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 8**
  - RACF:
    - Password phrases
    - IRRUT200 and IRRUT400 enhancements
    - SAF Identity Tokens for improved auditing
    - Virtual key ring support
    - DB2 V9 Support
  - DFSMS: Tape security enhancements
  - PKI Services:
    - Multiple Certificate Authority (CA) support
    - Simple Certificate Enrollment Protocol (SCEP) support
  - Communications Server
    - AES Support
    - IPv6 Enhancements

Agenda

- **z/OS Version 1 Release 7**
  - USER-related enhancements:
    - Mixed-case passwords
    - Detect or Prevent password recycling
    - Maintain revoke date when resuming users
    - Improve SETR INACTIVE processing for new users
  - Automatic RVARY SWITCH to backup for some errors
  - Support for the IBM Health Checker for z/OS
  - R_admin enhancements: New functions to extract USER, GROUP, and CONNECT information
  - Server Security Enhancements: Delegated Resources (AKA Nested ACEEs)
  - XML output for SMF Unload
  - Several PKI Services enhancements
  - Common Criteria certification

Agenda

- **z/OS Version 1 Release 6**
  - Dynamic Class Descriptor Table (CDT)
  - Password Enveloping and LDAP Change Log Support
  - Multilevel Security Auditing
- **z/OS Version 1 Release 5**
  - Dynamic RACF Templates
  - Multilevel Security
  - RACF Support for DB2 Version 8
  - PKI Services
  - Packaging

z/OS Security Server (RACF) Update

z/OS V1R8

RACF: Password Phrases

- RACF will allow you to specify a password phrase for a user:
  - 14 to 100 characters in length
  - Mixed-case, including alphabetic, numeric, and a large selection of special characters including blanks
  - Basic syntax rules: user ID can not appear in phrase; must contain at least two alphabetic and at least two non-alphabetic characters; must not contain more than two consecutive identical characters.
- Can provide:
  - better interoperability with other systems that allow longer passwords
  - better security than 8-character passwords
- Requires changes in applications that support passwords and want to support phrases
  - TSO/E, z/OS UNIX System Services, IMS, CICS, etc. will require changes
  - Changes will occur over time. Not in z/OS R8 for IBM applications.
- Users can have both a password phrase and a password
  - Will probably need both until all applications they use support phrases

RACF: IRRUT200 and IRRUT400 enhancements

- Problem 1: Database corruption will occur if
  - You use IRRUT200 or IRRUT400 with input DD and output DD pointing to same data set
  - You use IRRUT200 or IRRUT400 to copy into an active RACF data set
- Solution: Both utilities will now detect these conditions and terminate before performing the copy operation.
- Available as APAR OA14916 for z/OS R7.

RACF: IRRUT200 and IRRUT400 enhancements

Problem 2: When copying from primary into backup to resynchronize them you can lose updates:

- (1) IRRUT200 to copy from active primary to inactive backup;
- (2) some update happens (only to primary)
- (3) Use RVARY to activate the backup.

- **Solution: IRRUT200 now supports a new parameter, PARM=ACTIVATE**
  - If SYSRACF is an active primary, and SYSUT1 is the inactive backup, and PARM=ACTIVATE, then
  - IRRUT200 will issue an internal RVARY ACTIVE before it releases its database serialization.
  - Result: no updates can occur before the RVARY completes, and the backup and primary remain synchronized.

RACF: SAF Identity Tokens

- **Scenario:**
  - User logs on to a web server X as local user Y
  - Web server application sends request to z/OS, where it runs as z/OS user X
- **What identity do RACF audit records have?**
  - Answer: X
- **Is that what the auditor would like to see? Perhaps, but perhaps not.**
- **SAF Identity Tokens will allow better end-to-end auditing of user identity**
  - Applications can pass information about the original user to the destination system for auditing.
  - Similar to the X500name support that the z/OS HTTP server uses today for authentication via digital certificates

RACF: Virtual Key Rings

- Scenario:
  - z/OS user wants to use FTP to an SSL-enabled FTP server
  - Today each such user must have a certificate key ring containing the certificate of the trusted certifying authority (CA) that signed the server's certificate.
- Problem: Many users may want to use SSL-based client applications. All will need their own key rings, probably with identical contents, causing extra administration
- Solution: Virtual key rings
  - RACF will treat all the certificates that belong to a user as a key ring, without the administrator having to physically create a ring
  - Especially valuable for the case of certificates "owned" by the CERTAUTH user

RACF: DB2 V9 Support

- For improved security, DB2 V9 will support:
  - Trusted network connections
  - SQL "roles" that may be used to grant access to resources, rather than granting access to a user or group.
  - Specification of the role to use when a trusted server makes a DB2 request
- RACF support for DB2 will provide:
  - The ability of the security administrator to PERMIT access to DB2 resources when the request has a specific SQL role
  - DB2 exit and FASTAUTH changes to perform authorization checking based on the role name associated with the request

DFSMS: Tape Security Enhancements

- Today for tape security, you can use:
  - TAPEVOL profiles
  - DATASET profiles, with SETROPTS TAPEDSN
  - However, user can specify incorrect data set name unless you use:
    - TVTOC (tape volume table of contents) in TAPEVOL profiles to guarantee user specifies correct data set name
    - Or a tape management system that knows the right data set name
- Some concerns:
  - Management of TAPEVOL profiles can add administrative overhead
  - TVTOC processing limits the number of data sets on a tape
  - Users with access to some file based on the data set name may be able to access other files they should not have access to

IBM Systems and Technology Group

DFSMS: Tape Security Enhancements

- z/OS R8 will resolve those concerns, for systems with a compatible tape management system (such as DFSMSrmm)
- You can use new system-wide options in SYS1.PARMLIB(DEVSUPxx) to specify that:
  - The system will automatically check security for tape data sets using the DATASET class, even with SETR NOTAPEDSN and with the TAPEVOL class inactive (TAPEAUTHDSN option)
  - The system should treat tape security in a special way during migration from no tape security or TAPEVOL-based security to security based on data set names (TAPEAUTHRC4, TAPEAUTHRC8).
  - Users must have access to the data on file 1 of a tape (by data set name) before accessing a subsequent file (TAPEAUTHF1 option)

© 2006 IBM Corporation

PKI Services: Multiple Certificate Authority (CA) Support

- Today:
  - You can run only one instance of PKI Services daemon on a z/OS image
  - That single PKI Services daemon can act as (operate as) only a single certificate authority
- This makes it difficult to
  - Operate a certificate authority hierarchy
  - Host multiple certificate authorities as a service bureau
- z/OS R8: You can run multiple PKI Services daemons on one z/OS system
  - Each can operate as a different CA to resolve the above difficulties

PKI Services: SCEP Support

- Certificates are used by humans today, but increasingly also used by hardware (routers, VPN devices, etc.)
- Today, PKI Services accepts requests only via a web page
  - Leads to much manual work to get certificates for devices
- z/OS R8: PKI Services will accept requests via the Simple Certificate Enrollment Protocol (SCEP) directly from the devices, reducing the need for manual administrative actions

Communication Server

- **AES Support for IPSec**
- **IPv6 enhancements to support:**
  - **IPSec**
  - **IP Filtering**
  - **Internet Key Exchange (IKE) protocol**

z/OS Security Server (RACF) Update

z/OS V1R7

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…

- **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 Support for the IBM Health Checker for z/OS

- **What is the IBM Health Checker for z/OS?**
  - Originally a tool developed by ITSO to address component configuration and setup errors commonly made by installations
    - Web download
    - Implemented as a batch job
    - 37 checks
  - With z/OS V1R7, the IBM Health Checker for z/OS is integrated into z/OS
    - Implemented as a started task
    - 55 checks
    - Rolled back to z/OS V1R4 as a web download
    - Checks are shipped with components
    - Installations and vendors can write checks
    - Extensive SDSF support

RACF Support for the IBM Health Checker for z/OS…

- **RACF Support for the IBM Health Checker for z/OS:**
  - **New general resource classes: XFACILIT/GXFACILI**
    - The eXtended FACILITy class
    - Resource name of up to 246 characters
    - Shared POSIT value with the FACILITY class
    - Shipped in APAR OA10774, back to z/OS V1R4
  - **Two RACF checks:**
    - **RACF_GRS_RNL (rolled back to z/OS V1R6 with APAR OA11833)**
      - Checks to see if any of the RACF ENQ names are on a GRS resource name exclusion list which changes the scope of the RACF ENQ
    - **RACF_SENSITIVE_RESOURCES (rolled back to z/OS V1R4 with APAR OA11833)**
      - Looks at the current APF data sets and the RACF database data sets and flags those that are improperly protected
        - Are not found on the indicated volume
        - Are improperly protected

RACF_GRS_RNL Output

```
START TIME: 11/10/2004 10:13:10.341622  IBMRACF, RACF_GRS_RNL
OWNER DATE: 20040703

                        RACF_GRS_RNL Report

 S Major    Minor               Type  QName    Rname             Type
 - -------- ------------------- ----- -------- ----------------- ----
 E SYSZRACF SETROPTS            SERNL SYSZRACF SETROPTS          SPEC
 E SYSZRAC2 IRRCRV05            SERNL SYSZRAC2 IRRCRV05          SPEC
 E SYSZRAC2 IRRCRV05            SIRNL SYSZRAC2 IRRCRV05          SPEC

* High severity Exception *

IRRH202E   One or more RACF ENQ names were found in a GRS Resource Name
    List.

  Explanation:
    The RACF RACF_GRS_RNL check has detected that a RACF resource
    is covered by an entry in the specified GRS resource name list
    (RNL). RACF resource names should not be in either the system
    inclusion RNL (SIRNL) or the system exclusion RNL (SERNL).

  System Action:

    The check continues processing. There is no effect on the system.

...

  IBMRACF Reason: None of the RACF ENQ names should be in RNLs.
  Check parameters: N/A

END TIME: 01/08/2005 20:47:54.819710
```

RACF_SENSITIVE_RESOURCES Output

```
START TIME: 01/08/2005 20:47:54.701509  IBMRACF,
 CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
 START TIME: 04/14/2005 11:07:25.901856
 CHECK DATE: 20040703  CHECK SEVERITY: HIGH
 CHECK PARM: MARKN

                          APF Dataset Report

 S Data Set Name                          Vol    UACC Warn ID*  User
 - --------------------------------------- ------ ---- ---- ---- ----
 E SYS1.LINKLIB                           ZDR17  Read No   **** >Read
   SYS1.SVCLIB                            ZDR17  None No   None
 E ISPF350.ISPLOAD                        PRODAL Read No   **** >Read
 E ISPF350.ISPLPA                         PRODAL Read No   **** >Read
 E ISPF350.ISRLOAD                        PRODAL Read No   **** >Read
 E ISPF350.ISRLPA                         PRODAL Read No   **** >Read
 E ISPF350.LPALIB                         PRODAL Read No   **** >Read
 E RACF0001.ADAU.LOAD                     D94RF2 Updt Yes  ****
   RACF317.MIGLIB                         D97107
 V RACFTEST.RRSF.LOAD                     D94RF2

                        RACF Dataset Report


 S Data Set Name                          Vol    UACC Warn ID*  User
 - --------------------------------------- ------ ---- ---- ---- ----
   RACFDRVR.RACF317                       RDB317
* High severity Exception *

IRRH204E   The RACF health check RACF_SENSITIVE_RESOURCES has found one
    or more potential errors in the security controls on this system.
```


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

IBM Systems and Technology Group

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: Delegated Resources (AKA 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: Delegated Resources (AKA 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

XML Output for the RACF SMF Unload Utility

- **XML: The eXtensible Markup Language**
  - An industry standard way of tagging data
  - Simplifies data and document exchange
- **The RACF SMF Unload Utility (IRRADU00) now optionally produces XML-tagged output!**
  - XML output is created if the new DD names are allocated:
    - XMLOUT: Unformatted (long stream)
    - XMLFORM: Formatter (one tag/pair or field per record)
  - Type 30, 80, 81, and 83 events supported (including EIM)

XML Output for the SMF Unload Utility…

```
//SMFUNLD JOB ,'SMF DATA UNLOAD',
// MSGLEVEL=(1,1)
//SMFDUMP EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=A
//ADUPRINT DD SYSOUT=A
//SMFDATA DD DISP=SHR,DSN=USER01.RACF.SMFDATA
//XMLOUT  DD DISP=SHR,DSN=USER01.RACF.UNFORMAT.XMLADU00
//XMLFORM DD DISP=SHR,DSN=USER01.RACF.FORMAT.XMLADU00
//SYSIN DD *
  INDD(SMFDATA,OPTIONS(DUMP))
  OUTDD(SMFOUT,TYPE(000:255))
  ABEND(NORETRY)
  USER2(IRRADU00)
  USER3(IRRADU86)
/*
```

XML Output for the SMF Unload Utility…

- **Unformatted XML (XMLOUT DD)**

```
<event><eventType>ADDUSER</eventType><eventQual>SU……
```

- **Formatted XML (XMLFORM DD)**

```
<event>
  <eventType>ADDUSER</eventType>
  <eventQual>SUCCESS</eventQual>
  <timeWritten>21:51:55.54</timeWritten>
  <dateWritten>2005-01-17</dateWritten>
  <systemSmfid>IM13</systemSmfid>
  <prodFmid>HRF7720</prodFmid>
  <prodName>RACF</prodName>
  <details>
    <violation>N</violation>
Etc.
```

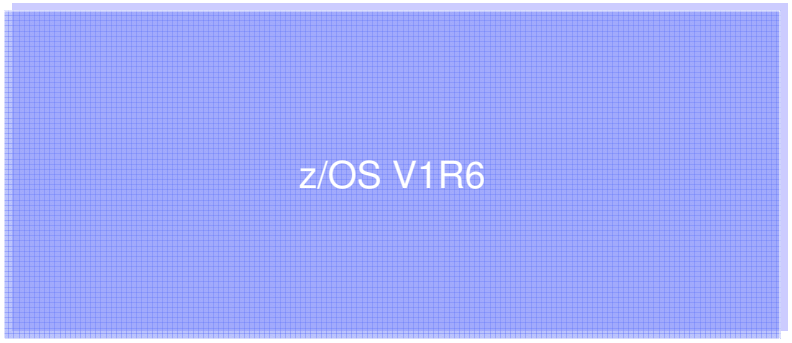

PKI Services Enhancements

- **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

Common Criteria

- **Common Criteria certification for z/OS R7 completed**
  - **Labeled Security Protection Profile (LSPP) at Evaluation Assurance Level 4 (EAL4)**
  - **Controlled Access Protection Profile (CAPP) at EAL4**
- **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 V1R7.0 Planning for Multilevel Security and the Common Criteria

z/OS Security Server (RACF) Update



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

What is Password Envelope / 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 V1R6 Multilevel Security Audit Enhancements

- **Multilevel Security Auditing (SECLABELAUDIT) enhancements**
  - Extends the auditing function of RACF to meet the Common Criteria auditing requirements for:
    - Labeled Security Protection Profile (LSPP) at Evaluated Assurance Level (EAL) 3+.
    - Controlled Access Protection Profile (CAPP) at Evaluated Assurance Level (EAL) 3+.
- **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)

z/OS Security Server (RACF) Update: V1R5

z/OS V1R5

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**
- **IRRMIN00 PARM=NEW no longer works against a RACF data set which is currently used by RACF on current system.**
- **SET LIST operator command displays the in-storage template level.**

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

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, this plug-in is 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**

PKI Services Enhancements with z/OS V1R5

- **PKI Services for z/OS V1R5 now certified as Identrus-compliant for certificate authority software**
- **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

IBM Systems and Technology Group

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 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**

Summary

- **z/OS Version 1 Release 8**
  - RACF:
    - Password phrases
    - SAF Identity Tokens for improved auditing
    - Virtual key ring support
    - DB2 V9 Support
  - DFSMS: Tape security enhancements
  - PKI Services:
    - Multiple Certificate Authority (CA) support
    - Simple Certificate Enrollment Protocol (SCEP) support
  - Communications Server:
    - AES
    - IPV6 enhancements

Summary

- **z/OS Version 1 Release 7**
  - USER-related enhancements:
    - Mixed-case passwords
    - Detect or Prevent password recycling
    - Maintain revoke date when resuming users
    - Improve SETR INACTIVE processing for new users
  - Automatic RVARY SWITCH to backup for some errors
  - Support for the IBM Health Checker for z/OS
  - R_admin enhancements: New functions to extract USER, GROUP, and CONNECT information
  - Nested ACEEs
  - XML output for SMF Unload
  - Several PKI Services enhancements
  - Common Criteria certification

Summary

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