RACF/LDAP Event Notification And Password Enveloping

Mike Onghena

RACF Development

onghena@us.ibm.com

Trademarks

- RACF
- z/OS

Agenda

- Objectives
- LDAP Event Notification
- Password Enveloping
- Externals
- Dependencies
- Migration Considerations

Objectives

- Allow RACF to participate in a multiplatform password synchronization solution such as one provided by IBM Directory Integrator (IDI).
- RACF was able to receive user and password updates from LDAP, but lacked the ability to notify anyone of updates.
- Support was added to allow RACF to notify LDAP of user and password changes.

LDAP provides

- Change log support for SDBM (RACF) backend
  - Enhanced PC interface for use by RACF
- LDAP interface to retrieve RACF password envelope

RACF provides

- Creation of LDAP change log entry (via LDAP's enhanced PC interface) when a USER profile or password changes in RACF
- Retrievable user passwords stored in RACF
- R_admin (IRRSEQ00) interface to retrieve encrypted password envelope
- R_Proxyserv (IRRSPY00) interface for applications to create their own change log entries

IDI provides

- 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.

RACF Event Notification

- Enabled by activating new RACFEVNT class and defining NOTIFY.LDAP.USER profile
- LDAP Change log entries created for changes to
  - a user's password, by any method
  - A user's revoke status (FLAG4 field), by any method
  - Other user fields (*) by the ADDUSER, ALTUSER, PASSWORD, and DELUSER commands
    - *exception: changes to group connection info not logged
- Application changes made using RACROUTE or ICHEINTY not logged
  - Application can call R_Proxyserv to create log entry

LDAP Change log entry contains

- Unique change log entry identifier
- Time and date of change
- Change type (add, modify, delete)
- Change initiator
- Change target

- Does not contain details of actual change (i.e. field names and values)
  - This is slightly different for password changes (described later)

Example

dn: changenumber=13,cn=changelog
objectclass: top
objectclass: changeLogEntry
objectclass: ibm-changelog
changenumber: 13
targetdn: racfid=JOEUSER,profiletype=user,o=ibm,c=us
changetype: modify
changetime: 20030729123000
ibm-changeinitiatorsname: racfid=JOEADMIN,profiletype=user,o=ibm,c=us

Password Enveloping

- LDAP change log entry is created to log the password update.
- New function allows authorized applications to recover a decryptable copy of the user's password.
- Scoped by user/group to allow only a subset of users to have retrievable passwords.
- Password enveloping is disabled by default for all users.

Password Enveloping

- In order to retrieve a user's password, all of the following must be true:
  1. The user whose password is to be retrieved must have authority to a RACFEVNT class profile in order to be eligible for password enveloping.
  2. The user or application requesting the password envelope must have authority to a FACILITY class profile in order to retrieve a password envelope.
  3. The user or application which retrieved a password envelope must decrypt it using a digital certificate with a private key which corresponds to a public key certificate in a RACF keyring owned by the RACF subsystem.

Big picture: Password update Part 1

ALTUSER BOB PASS(xxxxxx)

RACF

Public key encrypt new password for RACF only

PC to LDAP

RACF keyring

PC

LDAP

Create change log entry

IDI

Poll change log

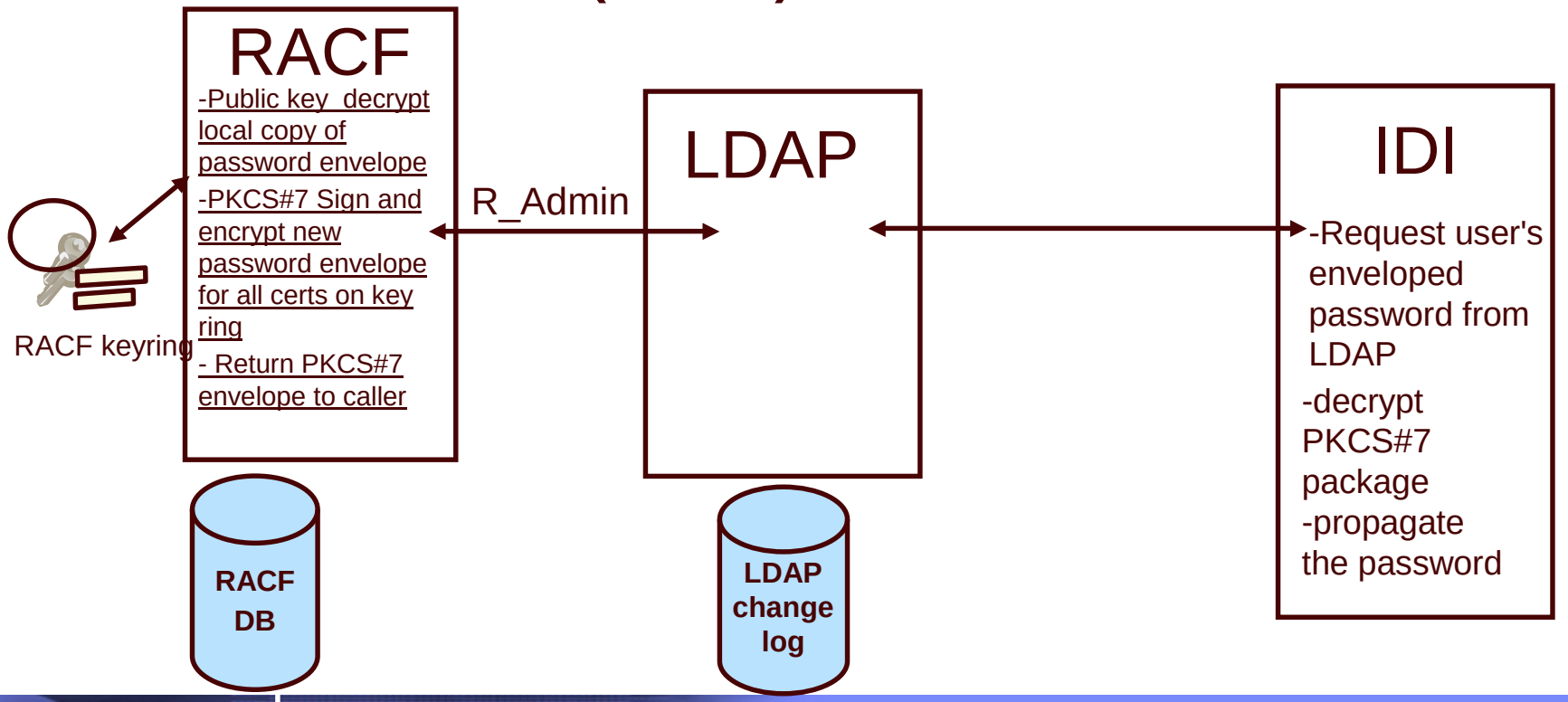
Detect password change

RACF DB

LDAP change log

Big picture: password update Part 2

ALTUSER BOB PASS(xxxxxx)



Contents of the password envelope

- Password ‘payload’ is first signed, then encrypted using PKCS#7 functions provided by System SSL
- Payload is BER-encoded ASCII. Password is lower case. ASN.1 format of the payload is

```
PasswordPayload ::= SEQUENCE{
    Version                 INTEGER
    Expired                 BOOLEAN
    Password                UTF8String
    Changetime              IA5String
    Language                IA5String  OPTIONAL DEFAULT "ENU"
 }
```

Setting up Password Enveloping

- Update RACF database templates
- Implement RACF subsystem address space (RASP) if not already implemented (it will be if you are already using LDAP to talk to RACF)
  - Define OMVS segment for RASP and its group(s)
  - If RASP not TRUSTED/PRIVILEGED, permit to IRR.DIGTCERT.LISTRING in the FACILITY class

Setting up Password Enveloping …

- Define Certificate Authority certificate to RACF
- Define Certificate and IRR.PWENV.KEYRING key ring for RASP
- Connect RASP cert to key ring as DEFAULT
- Define/import certificates for recipients (e.g. IDI) and connect them to key ring. Make sure they have TRUSTed status.

Setting up Password Enveloping …

- Define PASSWORD.ENVELOPE profile in the RACFEVNT class, activate RACFEVNT
  - Set APPLDATA to configure signature algorithm and encryption strength, or take defaults of MD5 and STRONG (168-bit triple DES)
  - Permit/exclude users and groups as appropriate. User's with READ access will have new passwords enveloped
  - RACLIST is optional
  - Need to STOP and restart RASP so UNIX System Services environment can be established
- Permit recipients to IRR.RADMIN.EXTRACT.PWENV in the FACILITY class

Setting up Password Enveloping …

- If LDAP notification of password changes is required, define NOTIFY.LDAP.USER profile in RACFEVNT (refresh RACFEVNT if RACLISTed)
  - Change log entry only created for password change if password is enveloped
  - Password change log entry contains ‘changes’ field which indicates that the password has changed, but does not include the actual password or envelope
  - If password and non-password data changed in the same command, e.g.

    ALTUSER JOE PASSWORD(NEWPW) RESUME OWNER(BOB)

    two separate change log entries are created

Sample change log entry for password change

dn: changenumber=13,cn=changelog
objectclass: top
objectclass: changeLogEntry
objectclass: ibm-changelog
changenumber: 13
targetdn: racfid=JOEUSER,profiletype=user,o=ibm,c=us
changetype: modify
changetime: 20030729123000
Changes: replace: racfPassword
racfPassword:*ComeAndGetIt*
ibm-changeinitiatorsname: racfid=JOEADMIN,profiletype=user,o=ibm,c=us

Some password changes are not enveloped

- For users who don't have READ access to PASSWORD.ENVELOPE
- Initial ADDUSER passwords
- When the new password is the same as the current password
- When the ALTUSER or PASSWORD command is used to change the password, and the new password is equal to the user's default group name
- When an application uses RACROUTE or ICHEINTY (as opposed to a RACF command) to set the password, and the password contains characters which would not be accepted by the RACF commands. RACF commands only accept the characters 'A'-'Z', '0'-'9', and the variant characters X'5B' (typically '$'), X'7B' (typically '#'), and X'7C' (typically '@').
- When an application uses RACROUTE or ICHEINTY to set the password and specifies ENCRYPT=NO

Summary of Externals

- Database Template updated to hold internal password envelope
- Database Unload report updated to report if a password envelope exists
- New RACFEVNT class
- New function code in r_admin (IRRSEQ00) to retrieve password envelope
- New function code in r_proxyserv (irrrspy00) to create changelog entry
- Update to RACF SET command to enable additional tracing.
- New and changed messages
- SAF mapping macro IRRPCOMP updated for callable service changes

Service levels

- Available now on z/OS Releases 3, 4 and 5
  - OA03853 – RACF updates
  - OA03854 – SAF updates
  - OA03857 – LDAP updates

Software Interdependencies

- RACF's LDAP notification is only meaningful if the SDBM back-end is configured in LDAP, and OA03857 is applied
- Pre-reqs to RACF APAR:
  - OW52135 (UW89972) - RACF SPE for UID/GID management (z/OS R3 only)
  - OW52480 (UW85562) - Corrective service to RACDBULD/TB (z/OS R3 only)
  - OA03076 (UA03883/UA03884) - Corrective service for IRRMPP00 (z/OS R3 and R4, respectively)
  - OW56905 (UW95429/UW95430) - Corrective service for IRRPCOMP (z/OS R3 and R4, respectively)
  - UW84120 - System SSL (z/OS R3 only)
  - UW84121 - System SSL strong encryption (z/OS R3 only)

Migration Considerations

- Use of the password enveloping function
  - Will utilize approx. 280 bytes of storage in the USER profile of eligible users
  - Requires the RASP to be a UNIX process
    - RASP initialization may complete later in the IPL sequence – after the OMVS kernel has initialized

Summary

- Objectives
- LDAP Event Notification
- Password Enveloping
- Externals
- Dependencies
- Migration Considerations

RACF/LDAP Event Notification And Password Enveloping

Mike Onghena

RACF Development

onghena@us.ibm.com