# IBM Education Assistance for z/OS V2R2

Item:  Password security enhancements
Element/Component: RACF

Material current as of May 2015

# Agenda

- Trademarks
- Presentation Objectives
- Overview
- Usage & Invocation
- Migration & Coexistence Considerations
- Installation
- Presentation Summary

# Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

# Presentation Objectives

- Recap of available password enhancements

- Understand the V2R2 enhancements being made for password security:
  - Removal of default password assignment on ADDUSER
  - Removal of masking default when there is no ICHDEX01 “password authentication” exit
  - Password phrase support for the RACLINK command
  - Default change for RACF_ENCRYPTION_ALGORITHM Health Check
  - ISPF panel support for the OA43999 SPE and the V2R2 enhancements

# Review – recent enhancements

- New Health Checks available via OA45608
  - RACF_ENCRYPTION_ALGORITHM
    - Checks that DES or KDFAES is active
  - RACF_PASSWORD_CONTROLS
    - SETROPTS INITSTATS active
    - SETROPTS PASSWORD(MIXEDCASE) active
    - SETROPTS PASSWORD(REVOKE(n)) <= 3
    - SETROPTS PASSWORD(INTERVAL(n)) <= 90

# Review – recent enhancements

- Available via OA43998 (SAF) and OA43999 (RACF):
  - Stronger encryption algorithm for passwords and password phrases
  - Special character support for passwords
  - Support for users to have a password phrase without also requiring a password
  - Ability to mark a password/phrase as expired without having to change its value
  - Password/phrase history clean-up function

- APAR documentation available at
  ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/oa43999.pdf
- Informational APAR II14765 documents restrictions and available service

# Usage & Invocation – Default password removal for ADDUSER

- 
- Problem Statement / Need Addressed
  - When ADDUSER is issued without the PASSWORD operand, the user's password defaults to the name of its default group
  - If the administrator forgets to change it in a timely manner, the password represents a guessable value that can be used to logon to the user
- Solution
  - The ADDUSER command no longer assigns a default password. If no phrase is specified, the user is defined as PROTECTED
- Benefit / Value
  - Remove a vulnerability resulting from a default behavior

# Usage & Invocation ...

- When the new default results in a PROTECTED user, a new informational message is issued:

```
ADDUSER NEWUSER
ICH01024I User NEWUSER  is defined as PROTECTED.
-
```

- The message is suppressed if NOPASSWORD is specified:

```
AU NEWUSER NOPASSWORD
```

- There is no message to indicate the lack of a password if a phrase is specified:

```
AU NEWUSER PHRASE('Making presentations is fun')
```

# Usage & Invocation – ICHDEX01 default change

- Problem Statement / Need Addressed
  - In the absence of an ICHDEX01 exit, RACF's default password evaluation behavior is to try first assuming DES, and if no match, try again using masking
  - Customers must activate an ICHDEX01 that requests only DES (rc=8)
  - The sample ICHDEX01 that RACF historically provided does not do this! It requests masking!
  -
  - Recall that when activating the new KDFAES password algorithm, masking is no longer used
  - However, what if you can't activate KDFAES, or you need to deactivate it?
- Solution
  - Change RACF default to use only DES for evaluation (when KDFAES not active)
- Benefit / Value
  - You can remove ICHDEX01 from your system unless you are implementing your own encryption

# Usage & Invocation …

- Migration Action: If you really have masked passwords, you need to change them, or install an ICHDEX01 exit that explicitly effects the previous default (rc=16)

- It is extremely unlikely you have masked passwords, however the RACF_ENCRYPTION_ALGORITHM Health Check shipped with OA45608 caught at least one client
  - In this case, a DES conversion is necessary, and the password-expire function available with OA43999 can be used to force password changes ASAP
  -

# Usage & Invocation – password phrase support for RACLINK

- Problem Statement / Need Addressed
  - OA43999 allows phrase-only users, but the RACLINK DEFINE command does not support phrases
  - Requirement to explicitly APPROVE a user association for a phrase-only user represents a loss of functionality
- Solution
  - Add phrase support to RACLINK DEFINE
- Benefit / Value
  - Remove RACF's last functional gap with phrases, thus eliminating another inhibitor to their adoption

# Usage & Invocation …

- The RACLINK DEFINE command allows specification of target user's password/phrase for implicit approval of the user ID association

```
RACLINK ID(thisuser) DEFINE(thatnode.thatuser/thatpwd) PEER(PWSYNC)
-
```

- Enclose the entire node.user/phrase string in single quotes if
  - the phrase starts with "*". Otherwise, TSO treats "/*" as a comment and ignores the rest of the command!
  - the phrase contains a space. Otherwise TSO treats the text after the space as another node.userid string
-

```
RACLINK DEFINE('NODE2.USER2/*This is my phrase') PEER(PWSYNC)

RACLINK DEFINE('NODE3.USER3/*This is your phrase'
  'NODE4.USER4/*This is his phrase') PEER(PWSYNC)
```

  - You may as well get into the habit of using single quotes for phrases

# Usage & Invocation – Default change for Health Check

- Problem Statement / Need Addressed
  - The RACF_ENCRYPTION_ALGORITHM Health Check shipped with OA45608 does not raise an exception if DES is the active algorithm
  - This was intentional for the SPE, but starting with V2R2, KDFAES should be considered the desirable/required algorithm
- Solution
  - Raise an exception unless KDFAES is the active algorithm
- Benefit / Value
  - Keep encouraging the use of more secure functions

# Migration & Coexistence Considerations

- Be aware of any scripts, test programs, etc that assume the assignment of a default password
- When sharing the RACF database
  - A user added on a downlevel system can still assign a default password, which will be recognized on the uplevel system
  - A user added on an uplevel system as PROTECTED by default will be recognized as PROTECTED on a downlevel system
- You can't use a password phrase on RACLINK DEFINE when establishing an association with a user on a downlevel system
  - It will appear to the downlevel system as though no password was specified, and the association will need to be manually APPROVEd on the downlevel system.

# Installation

- Consider removing your ICHDEX01 exit

# Presentation Summary

- There are additional password security enhancements beyond those introduced with OA43999
- ADDUSER default password removal and the ICHDEX01 default change are default behavior changes we did not feel comfortable making in the service stream
- Given that KDFAES will have been available for a while, the RACF_ENCRYPTION_ALGORITHM Health Check is being changed to raise an exception if it is not active on V2R2
- Password phrase support in the RACLINK APPROVE command removes RACF's final inhibitor to using phrases instead of passwords
  - Please (re)consider using password phrases instead of passwords where possible!