IBM Systems

NY RUG
October 2008

z/OS V1R10
Password Phrase Support

Eric Rosenfeld
Email Address: rosenfel@us.ibm.com

Trademarks

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

Session Objectives

- Describe changes related to Password Phrase support
  - Overview of updated support
    - How RACF changed
    - What changed in other components

What RACF Externals Are Affected?

- RACROUTE REQUEST=VERIFY allow PASSWORD=PassTicket and NEWPHRASE=, without requiring PHRASE=
- New field added to the User KERB segment (List only)
  - Reports on key source (password or password phrase)

Other RACROUTE Enhancements

- SETROPTS PASSWORD(WARNING(n)) support for password phrase
  - Now that TSO provides password phrase support in R10, wouldn't you like to see:

    ICH70002I YOUR PASSWORD PHRASE WILL EXPIRE IN 10 DAYS
- Lift the restriction that ICH70001I and ICH70002I are not returned when MSGRTRN= and ACEE= are specified on RACROUTE REQUEST=VERIFY/X
  - Informal customer requirements voiced
- Fail a "passthingy mismatch" instead of ignoring it
  - E.g. PASSWORD=,NEWPHRASE=, or, PHRASE=,NEWPASS=
  - Ignoring it leaves ambiguous behavior in applications like LDAP. User thinks his change was accepted, but it wasn't

How RACF Password Phrase Support Changed For Kerberos

- When an administrator or end user changes **either** a password or password phrase, this becomes the current Kerberos password and keys will be generated
- This is **consistent with other products' view, like TSO/E**, that the user has a 1-100 character password
- **As before, the end user is responsible for knowing that whenever the RACF "password" changes, the Kerberos password (and key) has also changed**

Migration & Coexistence Considerations

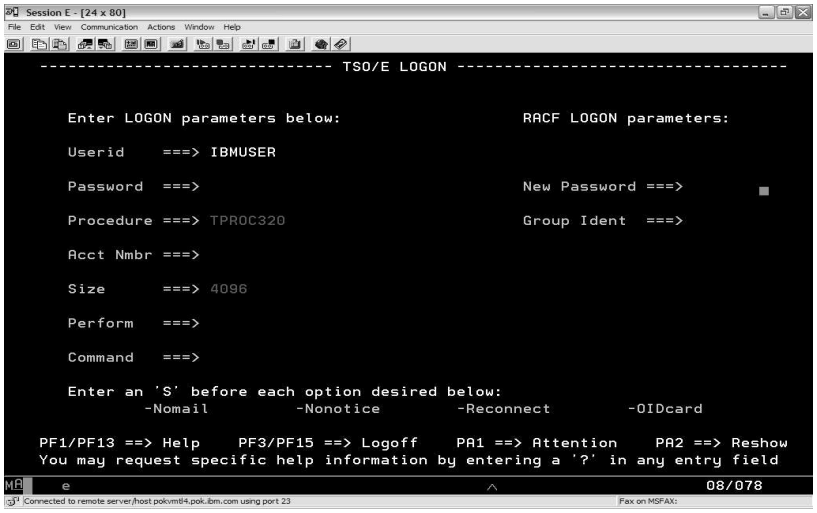
- Systems will require a toleration PTF to be installed for APAR OA22588 to ensure proper key processing for Kerberos
  - z/OS V1R6 UA39331
  - z/OS V1R7 UA39332
  - z/OS V1R8 UA39333
  - z/OS V1R9 UA39334

TSO/E Updates

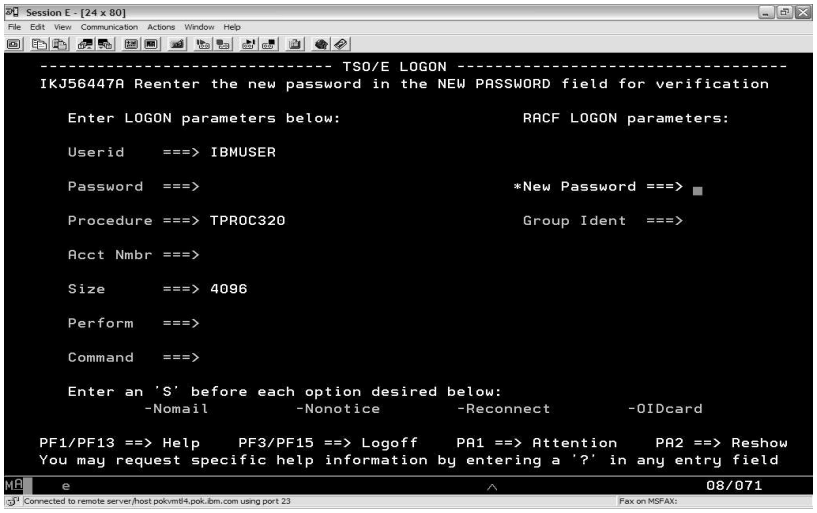
- Using this line item, the customer can:
  1. Logon with either a password or a password phrase
  2. Change the setting dynamically via an IKJTSOxx update
     - Activated by the following to the IKJTSOxx member:
       - LOGON PASSPHRASE(ON)

- Value:
  1. New panel still allows for eight character or less passwords
  2. Changes can be made without an IPL and easily displayed

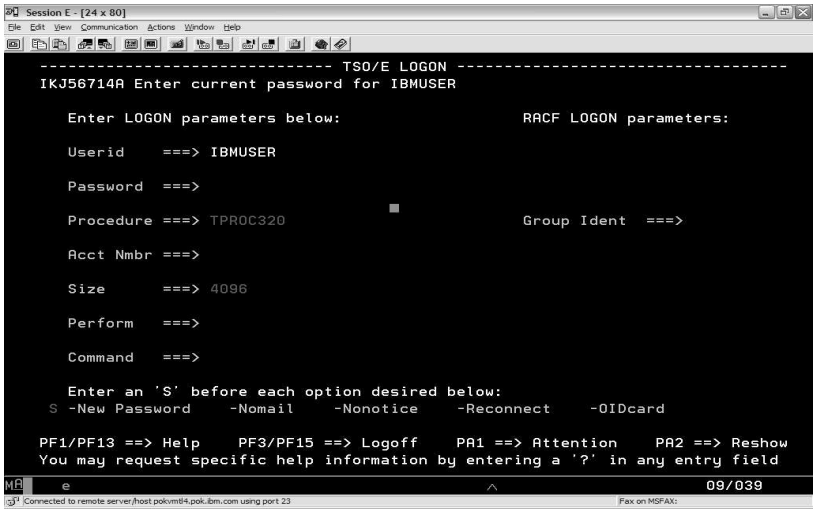
Password change with PASSPHRASE(OFF) – Step 1



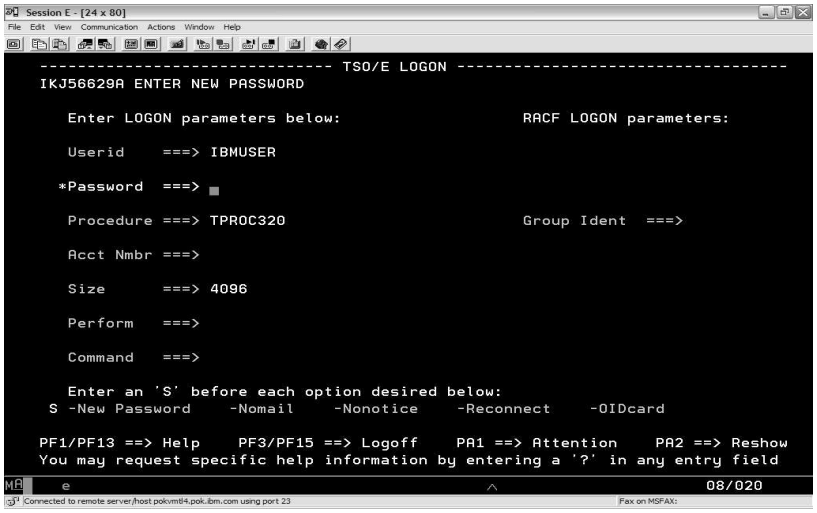
Password change with PASSPHRASE(OFF) – Step 2



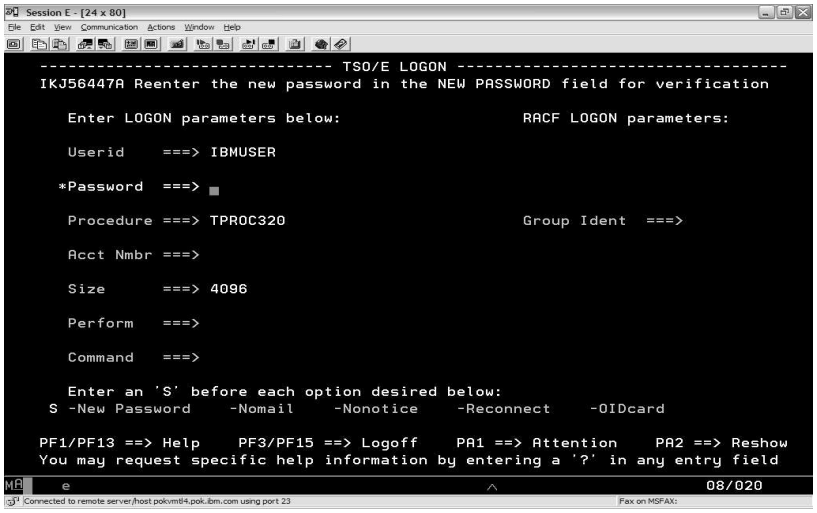
Password change with PASSPHRASE(ON) – Step 1



Password change with PASSPHRASE(ON) – Step 2



Password change with PASSPHRASE(ON) – Step 3



Migration & Coexistence Considerations

- Check logon exits (IKJEFLD, IKJEFLD1, IKJEFLN1, and IKJEFLN2)
  - Should allow 100 character passwords and new passwords
  - IKJEFLD also needs to allow for a new maximum size of 255
- Check any custom logon panels
  - Need to look at IKJLQENU not just IKJLPENU
- Toleration APAR OA20525 allows the new LOGON statement in the IKJTSOxx parmlib member to be ignored on lower levels and ensures correct output for the PARMLIB LIST ROUTE command
  - UA39737 (HTE7709)
  - UA39738 (HTE7730)
  - UA39739 (HTE7740)

UNIX System Services/LE

- Password phrase support is added to the following services
  - z/OS UNIX Assembler callable services
    BPX1PWD/BPX4PWD
    BPX1TLS/BPX4TLS
    BPX1SEC/BPX4SEC
  - C Functions
    __passwd() / __passwd_applid()
    pthread_security_np() / pthread_security_applid_np()
    __login() / __login_applid()

LDAP Password Phrase Use

- During bind
  - Can use a RACF password phrase instead of a password in any bind involving RACF
  - Can be changed specifying old and new phrase
- Changelog support
  - RACF creates separate changelog entry when password phrase changed
  - SDBM search specifying new **racfPassPhraseEnvelope** attribute retrieves password phrase envelope from RACF

Additional Updates

- Password phrase support is added to the following:
  - rlogin
  - passwd
  - su
  - OpenSSH

QUESTIONS?