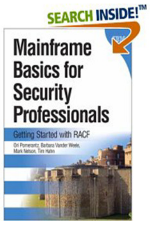
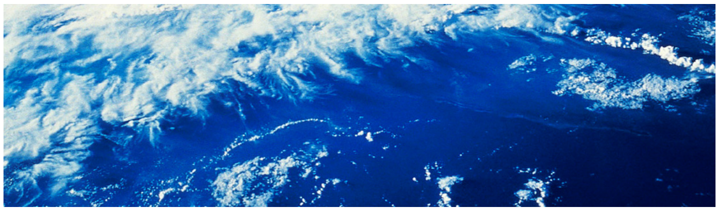
A Systems Programmer's View of OA43998/OA43999

NY Metro NaSPA
28 October, 2015

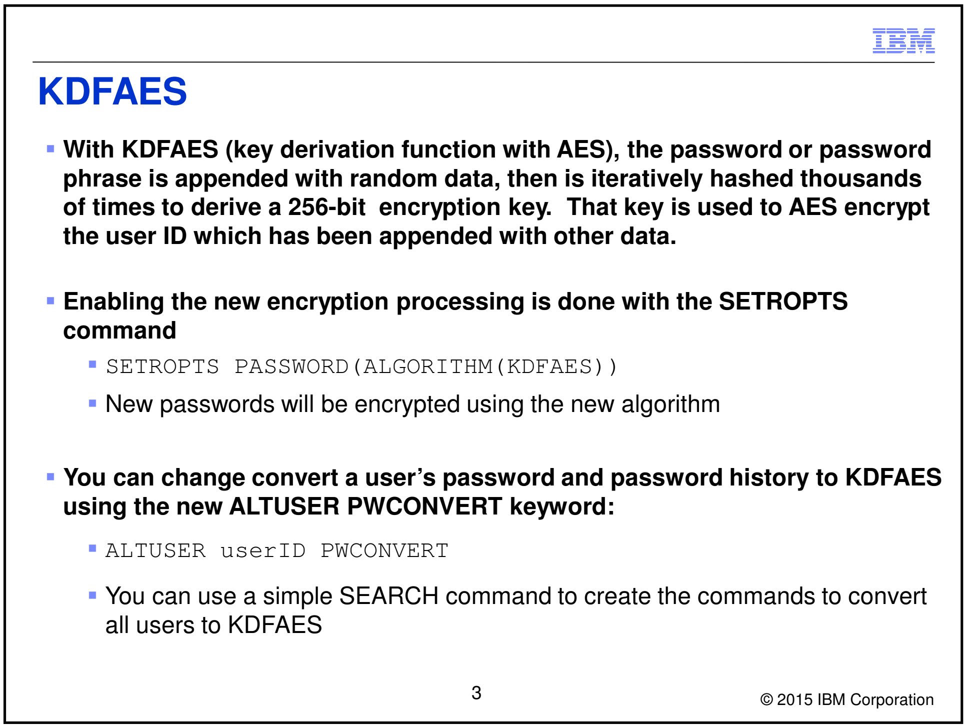
Mark Nelson, CISSP®, CSSLP®
RACF Design and Development
IBM Poughkeepsie
markan@us.ibm.com


SEARCH INSIDE!™
Mainframe Basics for Security Professionals
Getting Started with RACF



New Password Processing in RACF

- **New function APARs OA43998 (SAF)/OA43999(RACF)**
  - Migrate from 56-bit single key DES to key-derived AES (KDFAES)
  - Password-phrase-only users
  - Administrator password expiration
  - Password history cleanup
  - Additional "special" characters allowed in passwords
  - Rolled back to z/OS V1.12
- **A number of products are effected by these enhancements**
- **New SMP/E FIXCATEGORIES are defined for each function so that you can identify updates as they become available**
  - IBM.Function.RACF.PasswordEncryption
  - IBM.Function.RACF.PasswordCharacters
  - See http://www.ibm.com/systems/z/os/zos/features/smpe/fix-category.html for the complete list
- **Informational APAR II14765 documents known restrictions**

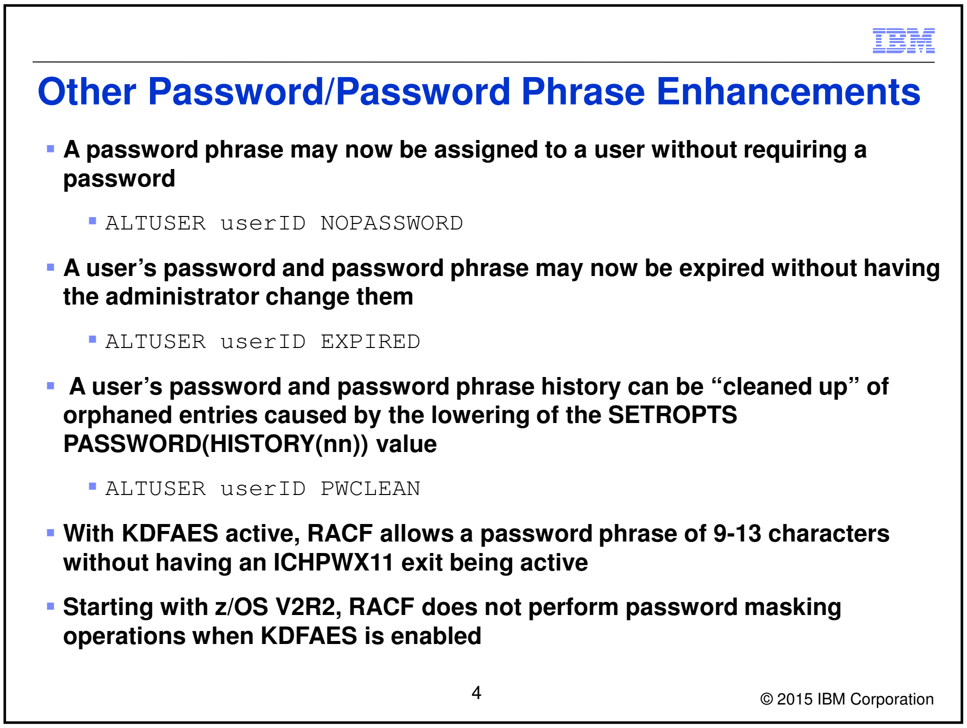


KDFAES

- **With KDFAES (key derivation function with AES), the password or password phrase is appended with random data, then is iteratively hashed thousands of times to derive a 256-bit encryption key. That key is used to AES encrypt the user ID which has been appended with other data.**

- **Enabling the new encryption processing is done with the SETROPTS command**
  - `SETROPTS PASSWORD(ALGORITHM(KDFAES))`
  - New passwords will be encrypted using the new algorithm

- **You can change convert a user's password and password history to KDFAES using the new ALTUSER PWCONVERT keyword:**
  - `ALTUSER userID PWCONVERT`
  - You can use a simple SEARCH command to create the commands to convert all users to KDFAES



Other Password/Password Phrase Enhancements

- **A password phrase may now be assigned to a user without requiring a password**
  - `ALTUSER userID NOPASSWORD`
- **A user's password and password phrase may now be expired without having the administrator change them**
  - `ALTUSER userID EXPIRED`
- **A user's password and password phrase history can be "cleaned up" of orphaned entries caused by the lowering of the SETROPTS PASSWORD(HISTORY(nn)) value**
  - `ALTUSER userID PWCLEAN`
- **With KDFAES active, RACF allows a password phrase of 9-13 characters without having an ICHPWX11 exit being active**
- **Starting with z/OS V2R2, RACF does not perform password masking operations when KDFAES is enabled**

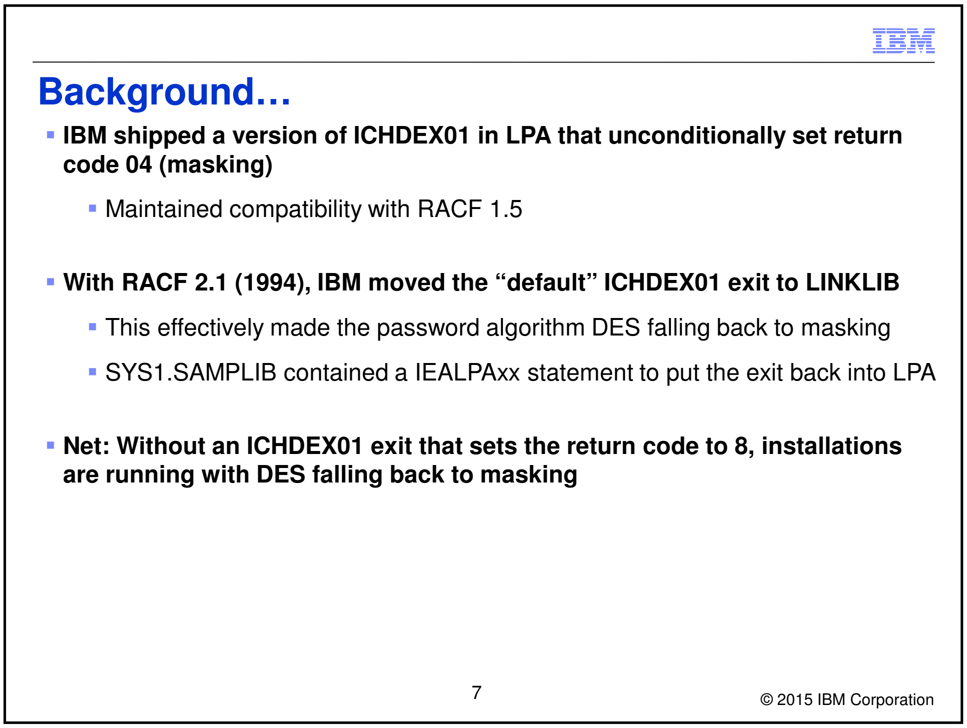
New Special Characters

- **New special characters are enabled with the SETROPTS command**
  - `SETROPTS PASSWORD(SPECIALCHARS)`
- **Two new values are available for your SETROPTS password rules:**
  - **SPECIAL**
    - Includes all of the new special characters plus the national characters ‘#’(X’7B’), ‘$’ (X’5B’) and “@” (X’7C’)
  - **MIXEDALL**
    - Allows all password characters
    - Can be used to force selections from each character grouping (upper case, lower case, numeric, and national/special) depending on the number of MIXEDALL positions and SETROPTS MIXEDCASE is in effect

<table>
<tr><th>Symbol</th><th>Hexadecimal Value</th></tr>
<tr><td>.</td><td>4B</td></tr>
<tr><td>&lt;</td><td>4C</td></tr>
<tr><td>+</td><td>4E</td></tr>
<tr><td>|</td><td>4F</td></tr>
<tr><td>&amp;</td><td>50</td></tr>
<tr><td>!</td><td>5A</td></tr>
<tr><td>*</td><td>5C</td></tr>
<tr><td>-</td><td>60</td></tr>
<tr><td>%</td><td>6C</td></tr>
<tr><td>_</td><td>6D</td></tr>
<tr><td>&gt;</td><td>6E</td></tr>
<tr><td>?</td><td>6F</td></tr>
<tr><td>:</td><td>7A</td></tr>
<tr><td>=</td><td>7E</td></tr>
</table>

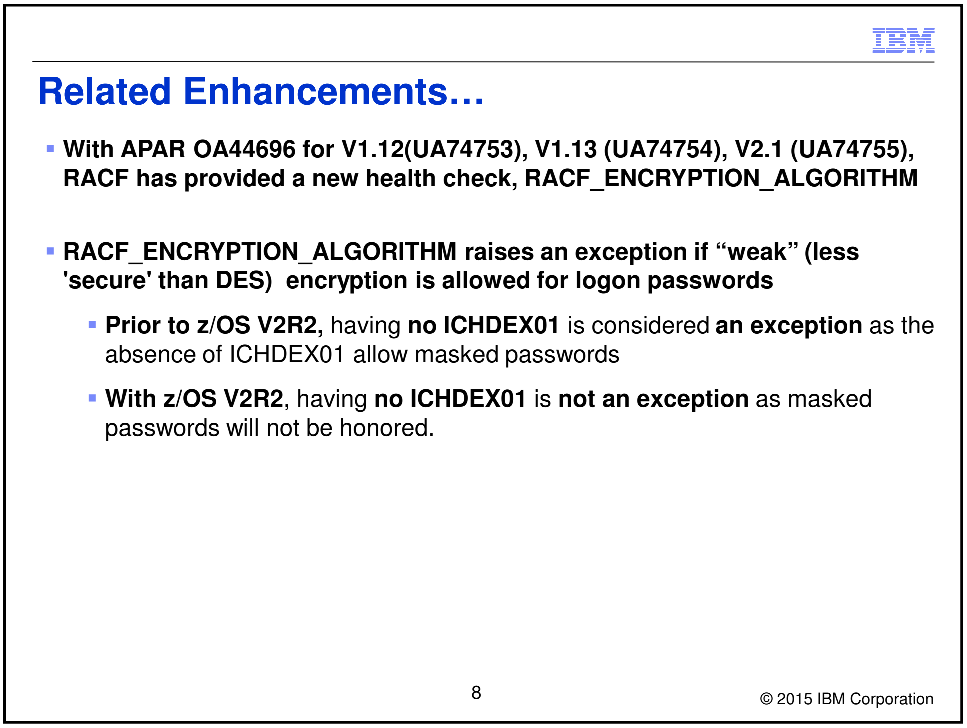
Background

- **Since its first release in 1976, RACF has supported the password as a primary authentication mechanism**
  - Originally, passwords were stored in a “masked” format
  - Reversible!
- **With RACF 1.6 (1984) RACF introduced a the “Data Encryption Standard” (DES) as an option for the storage of passwords**
  - Value stored in the RACF database is the user ID encrypted with the password
  - Not reversible, other than by “brute force”
- **The encryption algorithm was selected using a new exit, ICHDEX01, located in LPA**
  - Return code 04: Use masking algorithm
  - Return code 08: Use DES
  - Return code 16: Use DES, fall-back to masking
  - **No exit: Use DES than masking**



Background…

- **IBM shipped a version of ICHDEX01 in LPA that unconditionally set return code 04 (masking)**
  - Maintained compatibility with RACF 1.5
- **With RACF 2.1 (1994), IBM moved the “default” ICHDEX01 exit to LINKLIB**
  - This effectively made the password algorithm DES falling back to masking
  - SYS1.SAMPLIB contained a IEALPAxx statement to put the exit back into LPA
- **Net: Without an ICHDEX01 exit that sets the return code to 8, installations are running with DES falling back to masking**



Related Enhancements…

- **With APAR OA44696 for V1.12(UA74753), V1.13 (UA74754), V2.1 (UA74755), RACF has provided a new health check, RACF_ENCRYPTION_ALGORITHM**
- **RACF_ENCRYPTION_ALGORITHM raises an exception if “weak” (less 'secure' than DES) encryption is allowed for logon passwords**
  - **Prior to z/OS V2R2,** having **no ICHDEX01** is considered **an exception** as the absence of ICHDEX01 allow masked passwords
  - **With z/OS V2R2**, having **no ICHDEX01** is **not an exception** as masked passwords will not be honored.

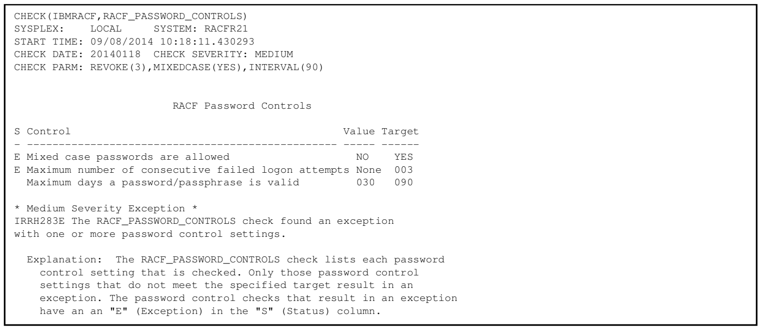
Related Enhancements…

- **RACF_ENCRYPTION_ALGORITHM exception summary:**

z/OS Release	**ICHDEX01**	**KDFAES Enabled**	**Result**
2.1 and earlier	Absent	No	Exception
2.1 and earlier	Present, DES only	No	No Exception
2.1 and earlier	Present, allows non-DES	No	Exception
2.1 and earlier	******************	Yes	No exception
2.2	******************	No	Exception
2.2	******************	Yes	No Exception

Related Enhancements…

- **RACF_PASSWORD_CONTROLS raises an exception if:**
  - Mixed case passwords are not in effect or
  - The maximum number of consecutive failed logon attempts is greater than 3 or
  - A password/password phrase can be valid for more than 90 days
- **All of the these values are set in a health check parameter**
- **Sample RACF_PASSWORD_CONTROLS output:**



```
CHECK(IBMRACF,RACF_PASSWORD_CONTROLS)
SYSPLEX:    LOCAL     SYSTEM: RACFR21
START TIME: 09/08/2014 10:18:11.430293
CHECK DATE: 20140118  CHECK SEVERITY: MEDIUM
CHECK PARM: REVOKE(3),MIXEDCASE(YES),INTERVAL(90)


                         RACF Password Controls

S Control                                             Value Target
- ------------------------------------------------- ----- ------
E Mixed case passwords are allowed                      NO    YES
E Maximum number of consecutive failed logon attempts None  003
  Maximum days a password/passphrase is valid          030   090

* Medium Severity Exception *
IRRH283E The RACF_PASSWORD_CONTROLS check found an exception
with one or more password control settings.

  Explanation:  The RACF_PASSWORD_CONTROLS check lists each password
    control setting that is checked. Only those password control
    settings that do not meet the specified target result in an
    exception. The password control checks that result in an exception
    have an an "E" (Exception) in the "S" (Status) column.
```

Implementation Considerations

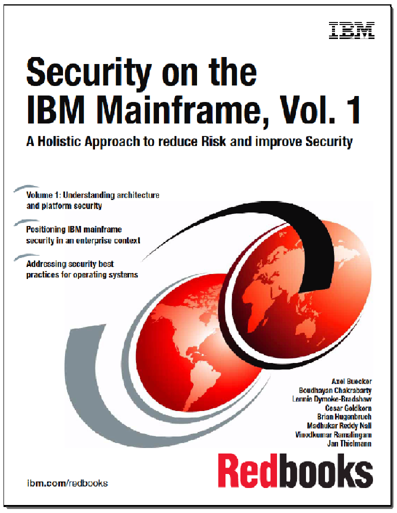
- **Before activating KDFAES or SPECIALCHARS, be sure to:**
  - Apply the OA43998/OA43999 PTFs on all systems sharing the RACF DB
  - Apply service to any products which are impacted by this new support
  - Verify that you have no “home grown” code which is affected
  - Determine the impact to your RACF exits (such as ICHDEX01/ICHPWX11)
  - Determine the impact to RACF “downloads” that you might use
  - Ensure that you have sufficient space in your RACF database to support the expansion of user profiles
  - For better performance, ensure that you are running on a processor which has the Central Processor Assist for Cryptographic Function (CPACF) to perform the SHA-256 operations.
  - Ensure that you are using ACEE caching in VLF (IRRACEE VLF class)
  - Ensure that your RRSF systems have OA43998/OA43999 applied and have consistent password settings
- **After activation, be sure to:**
  - Monitor your RACF DB for fragmentation and storage utilization

Shameless Plug: Hot Topics #29: August, 2015

- **Don’t Fall on your p@sSword**
- **Secure, but not foolproof**
- **Your order’s up! RACF client requirements satisfied in z/OS V2R2**
- **Erasure and encryption: The yin and yang of security technologies**
- **Drowning in digital certificates? Here’s a lifeline!**
- **Give credit to Crypto; It gives Crypto to Credit**
- **Fortify your SMF data with digital signatures**

Available at http://www.ibm.com/systems/z/os/zos/library/hot-topics/hot-topics.html

Helpful Publications



IBM

Security on the IBM Mainframe, Vol. 1

A Holistic Approach to reduce Risk and improve Security

Volume 1: Understanding architecture and platform security

Positioning IBM mainframe security in an enterprise context

Addressing security best practices for operating systems

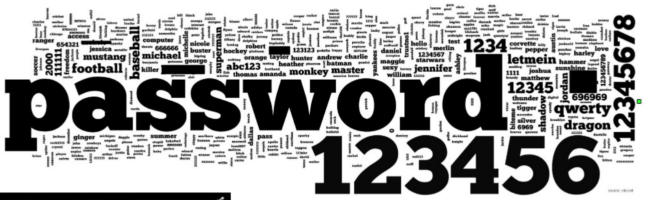
Axel Buecker
Boudhayan Chakrabarty
Lennie Dymoke-Bradshaw
Cesar Goldkorn
Brian Hugenbruch
Madhukar Reddy Nali
Vinodkumar Ramalingam
Jan Thielmann

ibm.com/redbooks

Redbooks

Caution!

- Left to their own, will users “do the right thing”?



https://www.youtube.com/watch?v=opRMrEfAIiI