Mark Nelson
RACF Design and Development
IBM Poughkeepsie

RACF® Update

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**

Background…

- **Ask yourself this question: “Which is a better encryption algorithm?” Your possible answers are:**
  - DES
  - AES
  - The question contains insufficient information to allow for a correct answer
- **The most important element in the question isn't the algorithm... it's the size and character set of the key!**
  - And what's the size of the key? It's the 8-byte password!
  - You can make the key space larger by enabling mixed-case passwords
- **Password phrases are a marvelous mechanism for resilience against brute force attacks.**
  - Wouldn't it be nice if you could have password phrase only users?
- **Resilience against brute-force password attacks is affected by**
  - The size and non-predictability of the key
  - The speed of the algorithm (***Faster isn't better***!)

The Paradox

- **Why does slowing down the encryption process help against a brute-force attack?**
  - You only have to do the algorithm once for a password validation.
  - The attacker has to do the algorithm once for each brute force attempt
  - The number of brute-force attempts needed is a function of the size of the key, the character set of the key…. and luck
  - **Net:** You are slowed down a little... the attacker is slowed down ***a lot!***

Other Challenges

- **RACF's password processing is very well known**
- **Some resource managers perform their processing knowing what RACF's processing is**
  - Some extract the cipher text password and then perform their own validation
  - Some present a ciphertext value during the authentication process
  - Some compute the ciphertext password themselves and insert that into the user profile
- **The challenge is to get all of these to work with whatever RACF implements**
  - Some vendor applications will have to change
- **Enablement must be optional**

The Statement of Direction

In the future, an enhanced RACF password encryption algorithm is planned. This support will be designed to provide improved cryptographic strength in RACF password algorithm processing. This will be intended to help protect RACF password data in the event that a copy of a RACF database becomes inadvertently accessible.

The Statement of Direction

In the future, **an enhanced RACF password encryption algorithm is planned. This support will be designed to provide improved cryptographic strength in RACF password algorithm processing. This will be intended to help protect RACF password data in the event that a copy of a RACF database becomes inadvertently accessible.**

The Statement of Direction

In the future, *an enhanced RACF password encryption algorithm is planned*. This support will be designed to provide improved cryptographic strength in RACF password algorithm processing. This will be intended to help protect RACF password data in the event that a copy of a RACF database becomes inadvertently accessible.

The Statement of Direction

In the future, an enhanced RACF password encryption algorithm is planned. This support will be *designed to provide improved cryptographic strength in RACF password algorithm processing*. This will be intended to help protect RACF password data in the event that a copy of a RACF database becomes inadvertently accessible.

The Statement of Direction

In the future, an enhanced RACF password encryption algorithm is planned. This support will be designed to provide improved cryptographic strength in RACF password algorithm processing. This will be intended to *help protect RACF password data in the event that a copy of a RACF database becomes inadvertently accessible.*

New Function

- **New function APARs OA43998 (SAF)/OA43999(RACF)**
  - Migrate from 56-bit single key DES to key-derived AES (KDFAES)
  - Password-phrase-only users
  - Administrative password expiration
  - Password history cleanup
  - Additional “special” characters allowed in passwords
  - Rollback to z/OS V1.12
  - A number of products are affected by these enhancements
- **New SMP/E FIXCATEGORIES are defined for each function so that you can identify updates as they become available**
- **Informational APAR II14765 will document known restrictions**
- **Detailed information can be found at https://ibm.biz/OA43999-Hold-Documentation**

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 and Password Phrase Improvements

- **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.**

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.

Symbol	Hexadecimal Value
.	4B
<	4C
+	4E
|	4F
&	50
!	5A
*	5C
-	60
%	6C
_	6D
>	6E
?	6F
:	7A
=	7E

Related Enhancements

- **RACF Database Unload Utility (IRRDBU00)**
  - User Basic Data (0200) record updated to contain:
    - The algorithm used to protect the password for the user
    - The algorithm used to protect the password phrase for the user
    - Legacy password history count
    - Legacy password phrase history count
    - KDFAES password history count
    - KDFAES password phrase history count
- **RACF SMF Unload Utility (IRRADU00)**
  - New keywords unloaded for ALTUSER, SETROPTS
  - RACF SMF type 81 initialization record new fields for SPECIALCHARS and encryption algorithm information

Related Enhancements…

- **With APAR OA45608 for V1.12(UA74753), V1.13 (UA74754), V2.1 (UA74755), RACF has provided two new health checks**
  - RACF_ENCRYPTION_ALGORITHM
  - RACF_PASSWORD_CONTROLS
- **RACF_ENCRYPTION_ALGORITHM raises an exception if “weak” (less 'secure' than DES) encryption is allowed for logon passwords**
  - Having no ICHDEX01 is considered an exception as the absence of ICHDEX01 allow masked passwords
- **Sample RACF_ENCRYPTION_ALGORITHM output when ICHDEX01 is absent:**

```
CHECK(IBMRACF,RACF_ENCRYPTION_ALGORITHM)
START TIME: 01/31/2014 09:44:29.892717
CHECK DATE: 20140131  CHECK SEVERITY: MEDIUM

IRRH295E  The RACF_ENCRYPTION_ALGORITHM check has detected an
exception. ICHDEX01 is not in use on this system. DES encryption
falls back to RACF masking.

END TIME: 01/31/2014 09:44:29.893680  STATUS: EXCEPTION-MED
```

Related Enhancements…

- **Sample Check output when ICHDEX01 is present with RC=8 (DES) only:**

```
CHECK(IBMRACF,RACF_ENCRYPTION_ALGORITHM)
START TIME: 01/31/2014 09:44:29.892717
CHECK DATE: 20140131  CHECK SEVERITY: MEDIUM

IRRH296I  ICHDEX01 is in use on this system.

              ICHDEX01 Return Codes

Installation Mask    DES      Installation  DES then  Other
Only         Only    Only     Only          Mask
(RC=0)       (RC=04) (RC=08)  (RC=12)       (RC=16)   (RC=OTHER)
------------ ------- -------  ------------- --------- ----------
NO           NO      YES      NO            NO        NO


IRRH297I ICHDEX01 indicates that only DES encryption is in use.

IRRH299I No exceptions are detected.

END TIME: 01/31/2014 09:44:29.893680  STATUS: SUCCESSFUL
```

Related Enhancements…

- **RACF_PASSWORD_CONTROLS raises an exception if:**
  - Mixed case passwords are not in effect or
  - The maximum number of consecutive failed logon attemps is greater than 3 or
  - A password/password phrase can be valid for more than 90 days
- **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.
```

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

A Look at z/OS Futures*

- This material is preliminary
- Work is in progress but not all designs/code are complete
- Some of what follows will change!
  - Some things might never appear, or appear (possibly *much*) later
  - Some things will be implemented differently as we go through Development
  - Some things will have different names and externals
  - And of course, some things will probably be added

*** Statements regarding IBM future direction and intent are subject to change or withdrawal, and represent goals and objectives only.**

Enhancing Security*

- **SMF record signing planned**
  - Idea is to make SMF a fully-trusted repository of audit data by making it much more tamper-evident
  - Designed to be available for SMF data written to System Logger
  - Planned to use both CPACF symmetric algorithm for hashing to support needed data rates and CEXnC card for signatures
  - Groups of records planned to be signed
  - Each group intended to have a new SMF2 trailer record with the signature
  - IFASMFDP support planned for verifying the signatures
    - To verify signatures:
      1. Unload using IFASMFDL
      2. Process the SMF data with IFASMFDP
  - We plan to document the SMF2 record format, so anyone can do signature verification

* Statements regarding IBM future direction and intent are subject to change or withdrawal, and represent goals and objectives only.

Enhancing Security*

- **PKINIT (RFC 4556) support planned**
  - Certificate-based authentication for Kerberos
- **RRSF Improvements**
  - Operator command-based dynamic movement of the MAIN system of an RRSF node planned
- **Separate OPERCMDS profiles for display/change aspects of F CATALOG**
  - Designed to support a new MVS.MODIFY.STC.CATALOG.CATALOG.SECURE profile
  - Will be intended to restrict access to the two different flavo of F CATALOG
    - READ access intended to allow display commands
    - UDPATE intended to allows changes to Catalog behavior

* Statements regarding IBM future direction and intent are subject to change or withdrawal, and represent goals and objectives only.

Enhancing Security*

- **More RACF Sensitive Resource Health Checks planned, for**:
  - RRSF work data sets
  - More z/OS UNIX System Services resources

- **Read-Only AUDITOR support will be designed to provide:**
  - A new ROAUDIT attribute intended to be a “look but don’t touch” setting
  - Designed to preclude changes to RACF audit events; otherwise, the same as AUDITOR
- **Console auto-logoff support planned:**
  - Designed to allow you to specify a timeout for consoles
  - Intended to be similar to timeouts for TSO/E and z/OS UNIX users
  - Automatically logging off unattended consoles is intended to help you improve security

* Statements regarding IBM future direction and intent are subject to change or withdrawal, and represent goals and objectives only.