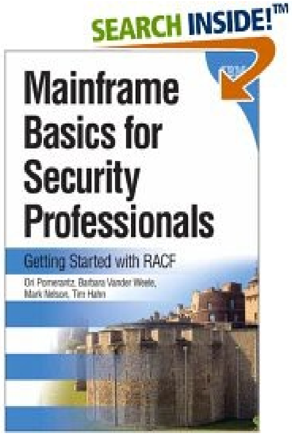
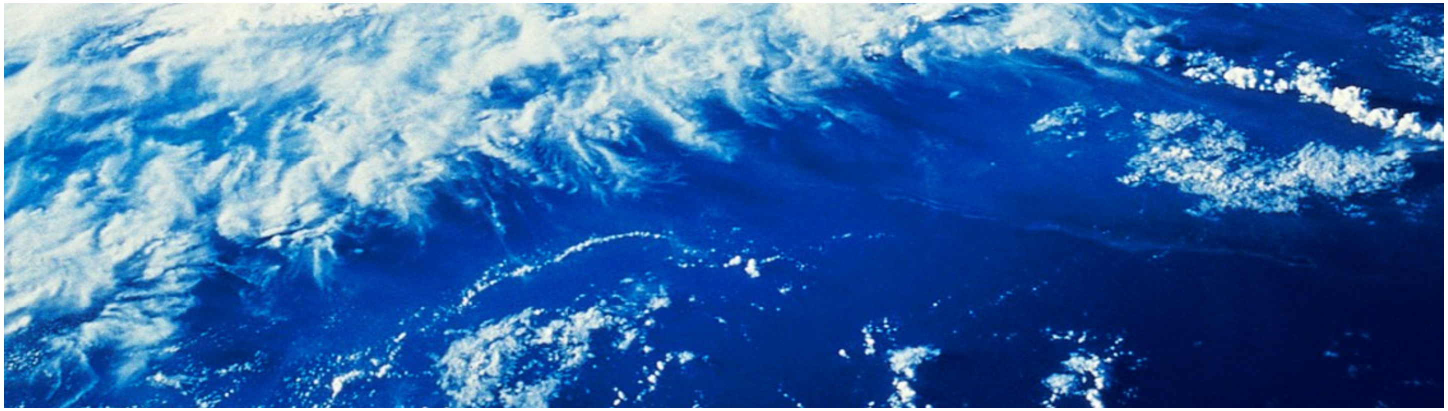
On the Horizon: How does RACF's Password Statement of Direction Affect Me?

Mark Nelson, CISSP®, CSSLP®
z/OS Security Server (RACF®) Development
IBM Poughkeepsie
markan@us.ibm.com

RACF Users Group of the North East
October 2014


SEARCH INSIDE!™
Mainframe Basics for Security Professionals
Getting Started with RACF
Ori Pomerantz, Barbara Vander Weele, Mark Nelson, Tim Hahn



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AIX*
BladeCenter*
BookManager*
CICS*
DataPower*
DB2*
DFSMS
DFSMSdss
DFSMShsm
DFSMSrmm
DFSORT

Domino*
DS6000
DS8000*
FICON*
IBM*
IBM eServer
IBM logo*
IMS
InfinBand

Language Environment*
MVS
Parallel Sysplex*
ProductPac*
RACF*
Redbooks*
REXX
RMF
ServerPac*

SYSREXX
System Storage
System x*
System z
System z9
System z10
System z10 Business Class
Tivoli*
WebSphere*

z10
z10 BC
z10 EC
zEnterprise*
zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Windows Server and the Windows logo are trademarks of the Microsoft group of countries.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

* Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Background

Authentication in RACF

- **The System Authorization Facility (SAF) supports several authentication mechanisms:**
  - 1-8 character password
  - 9-100 character password phrase
  - Pre-authenticated users, whose identity is mapped using
    - Digital certificate
    - Identity Propagation “token”
    - Application-specific mechanisms

- **RACF augments password processing with the PassTicket, an eight-character time-limited “password substitute” that is generated using a “shared secret” between the generating system and the evaluating system.**
- **Today, we'll be discussing the password and the password phrase**

Passwords in RACF

- **Passwords in RACF are not stored in the RACF data base**
- **RACF stores the cipher text that results from the user ID being encrypted with the password as a key**
- **Evaluating the password that has been submitted requires that the user ID be encrypted with the specified password and the resulting value compared against that which is stored in the RACF data base**
  - The entries in the password history are processed in a similar manner
- **RACF uses either the "original" RACF masking algorithm or DES, depending on the client's specification in ICHDEX01**
  - ICHDEX01 return code of 8 tells RACF to use DES. Any other return code does not force DES
  - Absence of ICHDEX01 causes RACF to use DES then the masking algorithm

The Statement of Direction

z/OS V2.1 RACF Statement of General Direction

- Enhanced RACF password encryption algorithm:
    - 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.

z/OS V2.1 RACF SOD: When

- Enhanced RACF password encryption algorithm:
  - ***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.

z/OS V2.1 RACF SOD: What (1)

- Enhanced RACF password encryption algorithm:
  - 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.

z/OS V2.1 RACF SOD: What (2)

- Enhanced RACF password encryption algorithm:
  - 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.

z/OS V2.1 RACF SOD: Why

- Enhanced RACF password encryption algorithm:
  - 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.***

What Does this Mean to Me?

Let's Get Philosophical

- **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
- **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!***)
- **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?

The Paradox

- **Why does slowing down the encryption process help against a brute-force attack?**
  - You only have to to 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... 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 whatever RACF implements**
  - Some vendor applications will have to change
- **Enablement must be optional**

On the Horizon

What's on the Horizon

- **New function APARs OA43998 (SAF)/OA43999(RACF)**
  - Migrate from 56-bit single key-derrived AES (KDFAES)
  - Password-phrase-only users
  - Administrator password expiration
  - Password history cleanup
  - Additional “special” characters allowed in passwords
  - Rollback planned 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
  - An informational APAR will document known restrictions

What's on the Horizon... Additional Characters

- **These characters are now allowed in a password:**

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

SMPE FIXCATEGORIES

- A **fix category** is an identifier used to group and associate PTFs to a particular category of software fixes.
  - A fix category might be used to identify a group of fixes that are required to support a particular hardware device, or to provide a particular software function, similar to how a preventive service planning bucket (PSP-bucket) identifies a group of PTFs.
  - Fix categories are supplied to you in the form of SMP/E FIXCAT HOLDDATA statements
- **IBM.Function.RACF.PasswordCharacters**
  - Fixes for z/OS Security Server RACF to support additional special characters in passwords, and fixes for other z/OS software to support this enhancement.
- **IBM.Function.RACF.PasswordEncryption**
  - Fixes for z/OS Security Server RACF to support a stronger password encryption algorithm, and fixes for other z/OS software to support this enhancement
- **A list of categories is at: http://www.ibm.com/systems/z/os/zos/features/smpe/fix-category.html**

Getting a Heads-Up: New RACF Health Check

- **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**

ICHDEX01 Installed	**ICHDEX01 Return Code Other than 8**	**New Encryption Enabled**	**Exception**
No	N/A	No	Yes: No ICHDEX01 means DES then masking
Yes	No	No	No
Yes	Yes	No	Yes, ICHDEX01 is requesting something other than DES
*	*	Yes	No

New Health Check: ICHDEX01 Not Installed

```
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
```

New Health Check: ICHDEX01 RC=8 Only (DES)

```
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
```

New Health Check: ICHDEX01 Non RC=8

```
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            YES       NO

* Medium Severity Exception *

IRRH298E ICHDEX01 indicates an encryption algorithm other than DES is in use.

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

New Health Check: New Encryption Algorithm Enabled

```
CHECK(IBMRACF,RACF_ENCRYPTION_ALGORITHM)

START TIME: 01/31/2014 09:44:29.892717
CHECK DATE: 20140131  CHECK SEVERITY: MEDIUM

IRRH294I  KDFAES encryption is enabled on this system. If present, ICHDEX01 is used
only for password history.

IRRH296I  ICHDEX01 is in use on this system.

              ICHDEX01 Return Codes

Installation DES     DES      Installation  DES       DES
Only         Only    Only     Only          Only      Only
(RC=00)      (RC=04) (RC=08)  (RC=12)       (RC=16)   (RC=OTHER)
------------ ------- -------  ------------- --------- ----------
NO           YES      NO      NO            NO        NO

IRRH299I No exceptions are detected.
END TIME: 01/31/2014 09:44:29.893680  STATUS: SUCCESSFUL
```

New Health Check: RACF_PASSWORD_CONTROLS

```
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.

    Use the SETROPTS LIST command to list the password control settings
    that are in effect. The SETROPTS command syntax is:

                             SETROPTS LIST
```

The Bottom Line

- The use of new new password encryption algorithm provides an improved defense against the disclosure of the contents of your RACF database

- Exploitation of the new support is recommended, but is optional.