My KDFAES Walkabout

Joel Tilton
RACF Engineer
Mainframe Evangelist
April 2016

About Joel Tilton

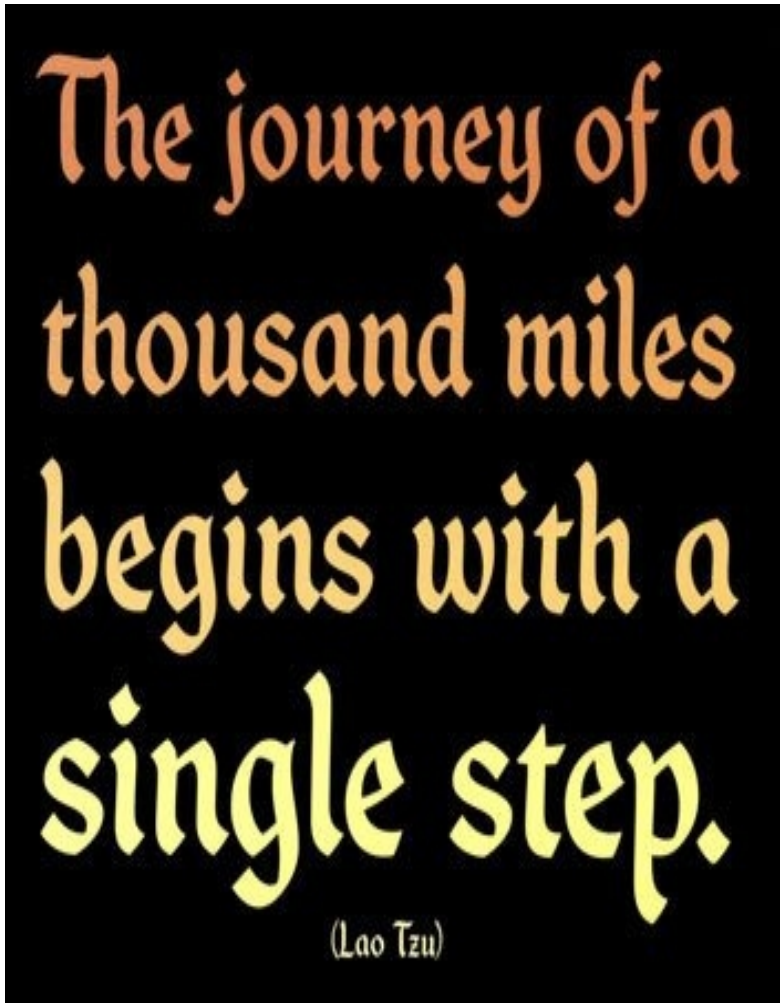
- Joel Tilton is a former employee of IBM, where he got his start with mainframes, who continues to champion mainframe security issues and solutions.
- Over 20+ years technical IT experience, the majority of which was gained in hands-on technical roles, performing a variety of duties in diverse and complex environments.
- The majority of Joel's experience is focused on IBM mainframe systems, where he performs as a Technician and Project Manager. Joel's specialist subject is IT Security, in particular z/OS and associated subsystems (CICS, DB2, MQ, zSecure, etc.) security with RACF.
- Joel is also an active member of the Tampa Bay RUG (RACF User Group) which meets jointly with the NY RUG. Joel has a true passion for security and the mainframe. Long live the mainframe!
- https://www.linkedin.com/in/joeltilton
- RACFEngineer@gmail.com
- 702-483-RACF (Google Voice)

Disclaimers

- All products, trademarks, and information mentioned are the property of the respective vendors.
- Mention of a product does not imply a recommendation.
- Always test new profiles on a non-production system.
- Only you can prevent IPLs…
- The views expressed are his own personal views, and are not endorsed or supported by, and do not necessarily express or reflect, the views, positions or strategies of his employer

Where to begin?

- RTFM
  - Read That Fine Manual!
- APAR OA43999 Doc
- Informational APAR
- RACF System Programmer's Guide
- RACF Security Administrator's Guide
- Redbook???



In the Beginning, there was Masking

- As the name *mask* implies it is very weak
- Validate no UserIDs have a masked value
  - z/OS 2.2 REQUIREMENT
  - Converting to KDFAES solves this problem
- Ideally ICHDEX01 is set to RC 08
- Use ICHPSOUT with PARM=DES
  - Attempts to de-mask a password before doing a DES encrypt operation
  - Writes error message if de-mask value contains any invalid password characters
  - DES encrypted password run through de-masking has a very high change of not having valid chars

Then Later, there was DES

- And the Data Encryption Standard was good…
- But as computing technology improved so did password cracking programs. Ugh!
- APAR OA43999 – RACF Password Security Enhancements
  - November 3rd 2014 Initial version
  - ftp://public.dhe.ibm.com/s390/zos/racf/pdf/oa43999.pdf
- Since when does shelf life of a PTF guarantee it is bug free?

Planning

- Biggest Issues:
  - Does Installed Software Support AES?
  - PTFs
- **II14765: SUPPORT INFORMATION REGARDING RACF PASSWORD SECURITY ENHANCEMENTS OA43998 AND OA43999**
  - http://www-01.ibm.com/support/docview.wss?uid=isg1II14765
- NetView FTP does not support the KDFAES encryption algorithm if the parameters SSECURP=('*','*') and/or RSECURP=('*','*') are used

Some Statistics

- Because everybody loves numbers…
- For 1k ALTUSER commands
  - Minimal Increase of 30 TCB seconds measured
- Why ALTUSER ?
- Does not VLF cache
- Every command costs full crypto overhead
- Good baseline measurement

PTF Highlights

- APAR OA43998 (SAF) & OA43999 (RACF)
- Two fix categories to track service updates
  - Run REPORT MISSINGFIX for Fix Categories
  - IBM.Function.RACF.PasswordCharacters
  - IBM.Function.RACF.PasswordEncryption
- zVM 6.3 support for KDFAES available with VM65719
- CICS 5.1 initial support PI21866
  - Additional Fixes: PI33454 & PI39336
- CICS 4.2 initial support PI21865
  - Additional Fixes: PI33451 & PI44380

Critical Planning Info

- PTFs Rollout ASAP ← Critical Path
- Enable VLF Caching ← Hard Requirement
  - The first logon of the day costs the most
- Plan for the size of the RACF DB to increase
  - AES encryption requires more physical space
  - Size of password and each password history entry more than doubles
  - In my testing a regularly reorganized DB at 48% used space increased to 53%
  - After "full" conversion
    - Full = password & password histories e.g. ALU PWCONVERT

CPACF REQUIRED

- Central Processor Assist for Cryptographic Functions
  - Accelerates the AES hashing functions
- Every mainframe "most likely" already has this on or you would have serious performance issues but…
- "Trust but Verify"
- Have your favorite sysprog that owes you a favor check the HMC (Hardware Management Console) ☺
- Check the output in the ICSF Address Space:
  - `CSFM126I CRYPTOGRAPHY - FULL CPU-BASED SERVICES ARE AVAILABLE.`
- REMINDER: ICSF must come up before PAGENT (AT TLS) or hardware acceleration will not be used

A Quick Word about ICSF & CPACF

- Both are independent of the other
- CPACF is a hardware feature enabled at HMC
- ICSF (Integrated Cryptographic Services Facility) accelerates encrypt/decrypt operations via CyptoExpress Cards
- You do not have to run ICSF address space to make CPACF available

ICSF Performance Improvement

- XFACILIT UACC(NONE) AUDIT(NONE)
  - They simply need to exist
- CSF.CSFSERV.AUTH.CSFOWH.DISABLE
  - Bypass SAF call for CSFSERV CSFOWH profile (one way hash)
- CSF.CSFSERV.AUTH.CSFRNG.DISABLE
  - Bypass SAF class for CSFSERV CSFRNG profile (random number generation)
- Example: SFTP, CSFOWH called for **every** packet sent & received! Uffda…
- Requires HCR77A1 release of ICSF at a minimum

- `CSFM650I CSFSERV AUTHORIZATION CHECK FOR RANDOM NUMBER GENERATE SERVICES IS DISABLED`

- `CSFM650I CSFSERV AUTHORIZATION CHECK FOR ONE-WAY HASH SERVICES IS DISABLED`

VLF Caching REQUIRED

- Did I mention VLF caching is

  REQUIRED
- First logon of the day costs
- SYS1.PARMLIB(COFVLFxx)
- CLASS NAME(IRRACEE) EMAJ(ACEE)
  - Cache ACEE in storage
- CLASS NAME(IRRGTS) EMAJ(GTS)
  - Cache RACF Group Tree

VLF Cache UNIX Related Info

- SYS1.PARMLIB(COFVLFxx)
- Cache UID & GID information too
  - CLASS NAME(IRRUMAP) EMAJ(UMAP)
  - CLASS NAME(IRRGMAP) EMAJ(GMAP)
  - CLASS NAME(IRRSMAP) EMAJ(SMAP)

To Convert or Not Convert

- Option 1 ← Because Your Mileage May Vary
  - SETR PASSWORD(ALGORITHM(KDFAES))
  - Wait for passwords to convert as time marches on
  - Do you have the time to wait?
- Option 2 ← Recommended
  - SETR PASSWORD(ALGORITHM(KDFAES))
  - ALU UserID PWCONVERT
    - Convert all password history entries up front

Passphrase Considerations

- ALU UserID PWCONVRT
  - Password Conversion Only
- How to convert a passphrase?
  - Change the password! ☹
- Suggested Strategy
  - ALU UserID NOPASSWORD
  - ALU UserID PWCLEAN
  - ALU UserID Phrase('myLongPasswordPhrase')

Backup Considerations

- Hopefully everyone is backing up their RACF DB nightly!!!
  - GDG limit 255
  - Why not, if it migrates anyway thanks to HSM
  - Modern VTS offers MIGRAT2 @ MIGRAT1 speeds!
  - Set course for fast recovery of tape,
    - Warp factor 9 Engage!

- A Strategy
  - Using zSecure backup all DES encrypted password values **BEFORE** you convert to KDFAES
  - CKGRACF ➔ APF authorized, TSO Authorized Command
    - Manipulate fields previously out of reach with RACF commands
      - LJDATE, LJTIME, previous & current password
    - Controlled by CKG.** in XFACILIT
- If *something* goes bump, then line item restore just that password

May I have this RVARY Dance?

- Another strategy…
- If you have password issues turn off KDFAES
- SETR PASSWORD(***NOALGORITHM***))
- Restore from the prior copy of the RACF DB
  - Issue: Now you have to forward recover any work you've done since the backup was taken
  - Ouch!!!!!!!!!!!!!
- Or issue ALU UserID EXPIRE to force the person to go back to a DES password
  - Not practical for non human IDs e.g. servers etc.

Helpful KDFAES features

- If you must turn off KDFAES
- SETR PASSWORD(***NOALGORITHM***))
- AES encrypted password histories will still evaluate!
  - Golf Clap RACF Development
- For systems using RRSF
  - Mixed Environment is ok
  - Meaning AES and DES encrypted RACF DBs can co-exist and passwords WILL sync.
  - Again Golf Clap RACF Development

New ALTUSER Keywords

- ALTUSER UserID PWCLEAN
  - Run this as you convert to AES
    - Because we like a squeaky clean RACF DB!
  - Ensure stale password history entries are gone
  - Raise your hand if you remember CUTPWHIS
  - Cost: Minimal time to build commands
- ALTUSER UserID EXPIRE ☺
  - Yes we can finally just expire a password

IRR401I

- `IRR410I RACF UNABLE TO BACK UP UPDATE OF xxxx after running ALU PWCONVERT`
- This does not mean the RACF DB is corrupted
- To date this is the only technical hiccup I have experienced
- Solution
  - RVARY INACT DATASET(backup dataset name)
  - Sub UT200 job with PARM=ACTIVATE

Idea!

- So based upon receiving IRR410I you could:
- RVARY INACT DATASET(backup dataset name)
- Run batch job with ALU UserID PWCONVERT
- Sub UT200 job with PARM=ACTIVATE
- Why?
  - Well since we know about an IRR410I potential why not?
  - Batch job with PWCONVERT runs faster without the backup online

Sample Production DB Stats

Before AES	After AES	Delta	UserIDs
48%	54%	6%	40k+
45%	51%	6%	40k+
37%	44%	7%	35k+

- Not Split
- Plan for RACF DB Size Increase
  - AES Password more than doubles password field
- Recommend reorg after full AES conversion

zSecure Command Verifier

- You might want to consider defining
- C4R.RACF.USER.PASSWORD.ALGORITHM
- C4R.RACF.USER.PASSWORD.SPECIALCHARS
- UACC(NONE) AUDIT(ALL(READ))
- Empty Access List
- Prevent the SETR command until you are ready to implement

Summary

- Try not. Do…or do not. There is no try!
  - Master Yoda
- How do you tackle any project? One small step at a time…
- Study Info APAR and APAR OA43999 doco
- Get Needed PTFs rolling out ASAP
- Validate CPACF Enabled
- Plan a backout strategy
- Rehearse backout strategy
- Implement
- AES Password Encryption Engage!

My Thanks To…

- Stu Henderson
- Adam Klinger
- Mark Nelson
- Kevin Shelton
- Hayim Sokolsky
- William Vender
- Bruce Wells

- And the Adventure Continues to Boldly Go Where No Encryption Algorithm Has Gone Before …

Questions?

What is KDFAES

- A stronger encryption algorithm that makes it much harder to brute force attack passwords stored in RACF.
- https://www.ibm.com/support/knowledgecenter/SSLTBW_2.2.0/com.ibm.zos.v2r2.icha200/icha20079.htm

APAR OA43999 Doc

- ftp://public.dhe.ibm.com/s390/zos/racf/pdf/oa43999.pdf

Planning Docs

- PLANNING CONSIDERATIONS
- https://www.ibm.com/support/knowledgecenter/SSLTBW_2.2.0/com.ibm.zos.v2r2.icha200/icha20091a.htm

- RACF UPDATE Presentation from Mark Nelson
- ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/nyrug_2014_11_racf_update.pdf

VLF Caching Doc

- https://www.ibm.com/support/knowledgecenter/SSLTBW_1.13.0/com.ibm.zos.r13.icha200/ichza2c043.htm%23wq178
- https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.bpxb200/stepcac.htm

CPACF Doc

- https://www.ibm.com/support/knowledgecenter/linuxonibm/com.ibm.linux.z.wskc.doc/wskc_c_so2cpacf.html