Why Complex Passwords Should Be Fact and Not Fiction

December 2017 Update

Presented by

Richard K. Faulhaber

rkf@newera.com twitter: @faulhaber_rk

Introduction: Who am I?

A technical person with a creative background.

Science and the arts - Eclectic education and interests.

Chemistry Lab, Research, Libraries, Banking, IT/Office Management, Tech Support.

Creative solutions to technical problems.

Visualization of RACF Password Symbols paper.

SHARE Speaker: San Antonio & Atlanta ’16
San Jose & Providence ’17
Sacramento ’18

Overview:

- Why complex passwords are important.
- Results of the latest survey.
- Password mechanics / mathematics.
- Tools for creating strong, complex, (nearly) un-guessable passwords.

** All of this applies to password phrases, as well.

What are passwords and why are they important?

- "Passwords are our most basic way of proving who we are to a computer. By implication, this is also how we control who can use our computer."

  - Stu Henderson *

- Passwords ***help*** protect systems from unwarranted access.

  Systems with which we interact *SHOULD* have a number of safeguards in place to prevent unwarranted access. These safeguards fortify the WALLS of the kingdom's castle.

- Your UserID and password represent the keys to the kingdom.

* The Mainframe Audit News, Issue 14, March 2010 - How to Think About Passwords and How to Think Deeply About Passwords
http://www.stuhenderson.com/Mainframe%20Audit%20News/MANEWS14.pdf

What are passwords and why are they important?

- The USER (with a capital Y – O – U) holds these keys.

People are the weakest link…

81% of hacking-related breaches leveraged either stolen and/or weak passwords. *

- Practice cyberhygiene: “all those annoying things, such as using long and complex passwords and changing them frequently.” **

* Verizon’s 2017 Data Breach Investigations Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

** Former NATO Commander Says Cybersecurity Most Worrying Threat We Face - by Tim Stafford, October 30, 2017
https://www.gartner.com/smarterwithgartner/former-nato-commander-says-cybersecurity-most-worrying-threat-we-face/

What are passwords and why are they important?

- Not everyone agrees on what makes a good password *
- NIST recommendations **

* Want stronger passwords? Understand these 4 common password security myths - By Fahmida Y. Rashid, Senior Writer, CSO, OCT 3, 2017
https://www.csoonline.com/article/3228106/password-security/want-stronger-passwords-understand-these-4-common-password-security-myths.html

** NIST recommendations (link to be added)

What are passwords and why are they important?

- Professional integrity: you wouldn’t leave sensitive documents or a company laptop sitting on the front seat of your car…

- Likewise, you shouldn’t be lazy when it comes to your passwords.

New Technologies

Two Factor Authentication

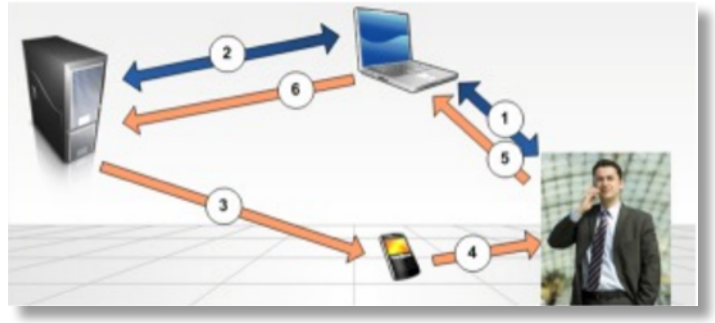
Multi-Factor Authentication

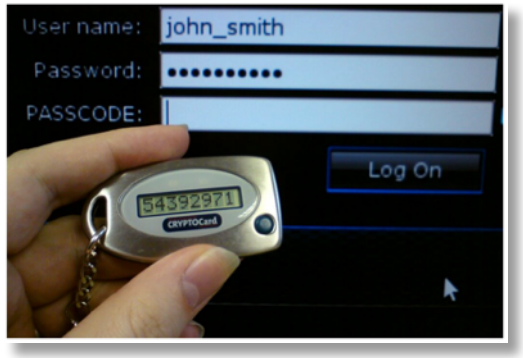
Smart Cards

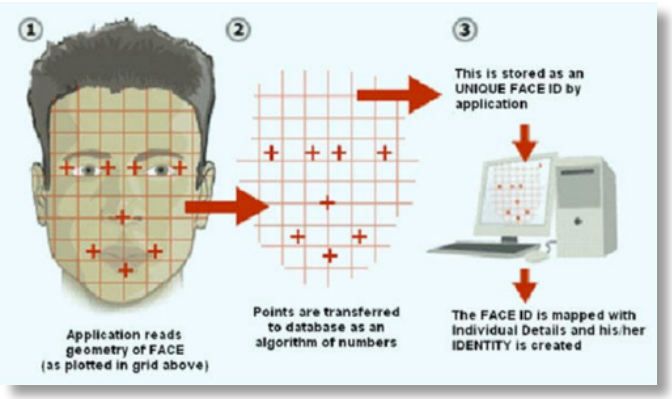
Touch Tokens

Secure IDs

Biometrics







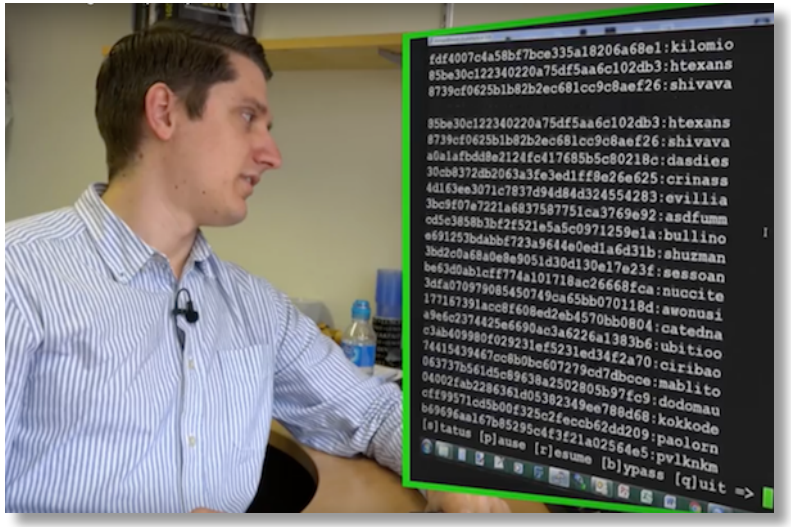
Encryption

Are you using KDFAES to encrypt your database?

- WHY NOT?
- DES is broken. *
- Password Cracking in Action:

  From the Computerphile YouTube Channel

  https://youtu.be/7U-RbOKanYs



Dr. Mike Pound – Computer Science at the University of Nottingham.

* Password Cracking and Self-Encrypting Drives, Chad Rikansrud, RSM Partners, September 2017
http://www.newera-info.com/CR1.html

Worst case scenario:

- RSA Secure Keyfob - stolen
- Smartcard - stolen
- Email - hacked
- Cellphone - stolen & hacked*
- Biometrics - spoofed ?!?**

* That Fingerprint Sensor on Your Phone Is Not as Safe as You Think, By VINDU GOEL, APRIL 10, 2017
https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html?_r=0
** This $150 mask beat Face ID on the iPhone X - by Thuy Ong@ThuyOng Nov 13, 2017
https://www.theverge.com/2017/11/13/16642690/bkav-iphone-x-faceid-mask

Worst case scenario:

- Multi-Factor authentication gets nocked down a factor when your password is:
  - Simple
  - Short
  - Common
  - Guessable
  - Shared
  - Reused
- ESM database - stolen

MFA – not yet implemented

Password Phrases – not yet activated

Additional Special Symbols – not in use

Mixed Case – not allowed

Recent Survey Results:

1. Which ESM?

RACF – 75% ACF2 or TSS – 25%

2. Is AES implemented?

YES – 37% Compared to 5% last year.

3. Mixed case / lower case implemented?

YES – 44% Compared to 22% last year.

4. Additional Special symbols implemented?

YES – 44% Compared to 16% last year.

5. Password Phrases implemented?

YES – 50% Compared to 14% last year.

6. Password Rules or Mask implemented?

YES – 81%

7. Augmented authentication in use?

YES – 43%

SIGNIFICANT INCREASES TO AUTHENTICATION SECURITY!

Password Mechanics:

- Maximum length for mainframe passwords: 8 symbols

```
p@ssword
12345678
```

- Password phrases length spans from 9 to 100 symbols:
  - 9 to 100, if password phrase exit (ICHPWX11) is present,
  - 14 to 100, if password phrase exit (ICHPWX11) is not present

```
p@sswordpa5$wordP@ssw0rdPa55wordpA$$WorDpasswOrdp@sswordp@sswordp@sswordpa5$wordP@ssw0rdPa55word2017
12345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890
```

Password Mechanics: Three Elements

- **Length = STRENGTH**

- **Symbols available for use - MORE** is better than **LESS**

  Defaults: A-Z 0-9 #$@ (39 symbols)

Up to 5.3 TRILLION possible password combinations!

- **Longevity**

  Number of days a password is valid:

  RACF: range: 1-254; default=30
  ACF2: range: 0-255; default=0
  TSS: range: 0-255; default=30

Password Mathematics:

Search Space is the total number of possible password combinations given:

- a set of symbols
- a length

Symbol Combination Statistics - **Safety in Numbers**

- Search Space Formula:

  N*N*N*N*N*N*N*N or N^P

- Length 8 – all numeric:

  10*10*10*10*10*10*10*10 or 10^8 = 100,000,000 possible passwords

- 00000000, 00000001, 00000002, etc… 99999999

Password Mathematics:

Symbol Combination Statistics - **Safety in Numbers**

- Length 8 – alphanumeric (A-Z 0-9 #$@)
  39 symbols available
  $39*39*39*39*39*39*39*39$ or 39^8 =
  5,352,009,260,481 possible passwords

- Length 8 – alphanumeric, lower case
  (A-Z a-z 0-9 #$@)
  65 symbols available
  $65*65*65*65*65*65*65*65$ or 65^8 =
  318,644,812,890,625 possible passwords

Password Mathematics:

Symbol Combination Statistics - **Safety in Numbers**

- Length 8 – alphanumeric, lower case,
  special chars (A-Z a-z 0-9 #$@ .<+|&!*-%_>?:=)
  79 symbols available
  $79*79*79*79*79*79*79*79$ or 79^8 =
  1,517,108,809,906,560 possible passwords

Password Mathematics:

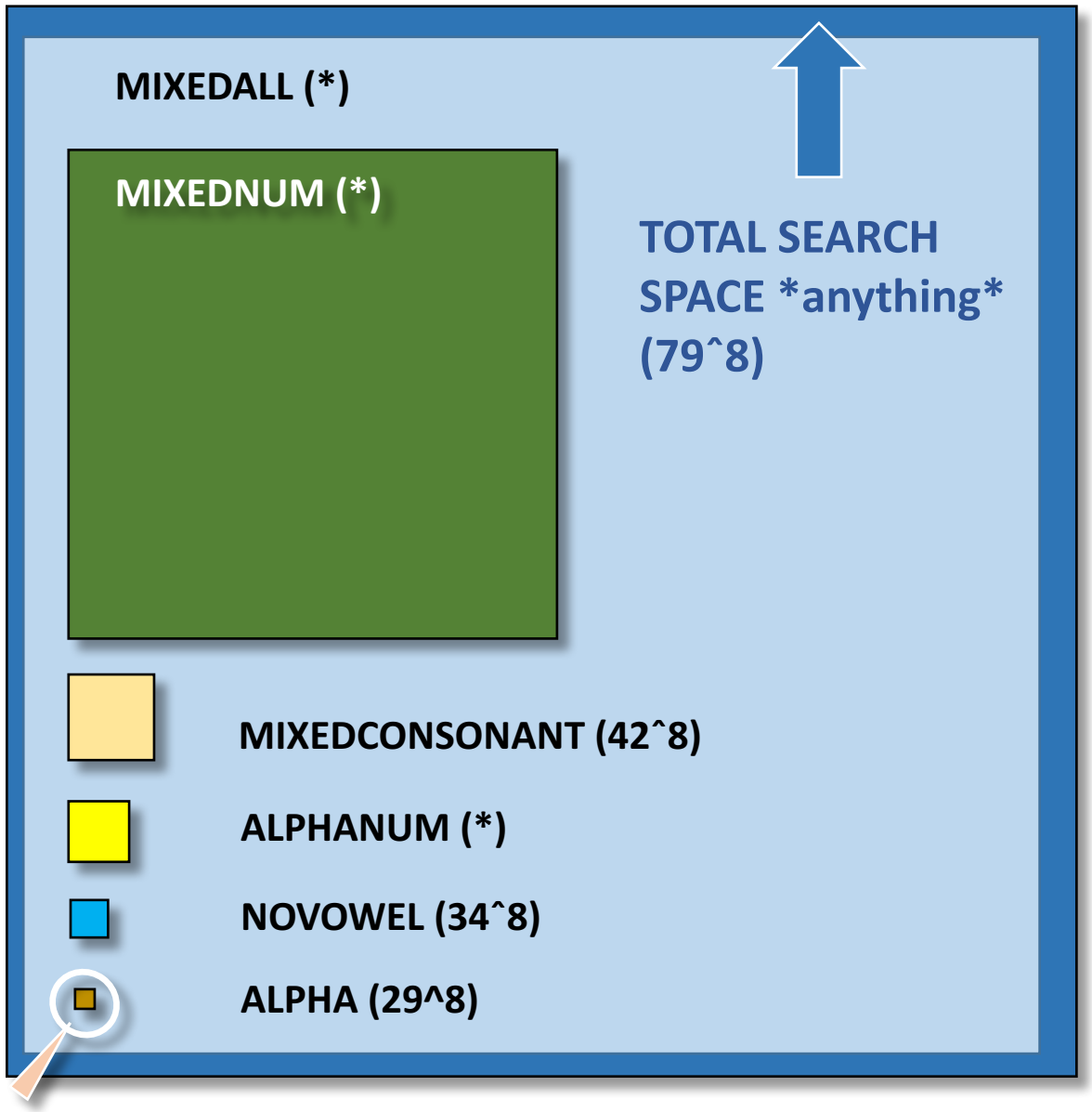
Symbol Combination Statistics - **Safety in Numbers**

Visual representation of symbol sets based on:

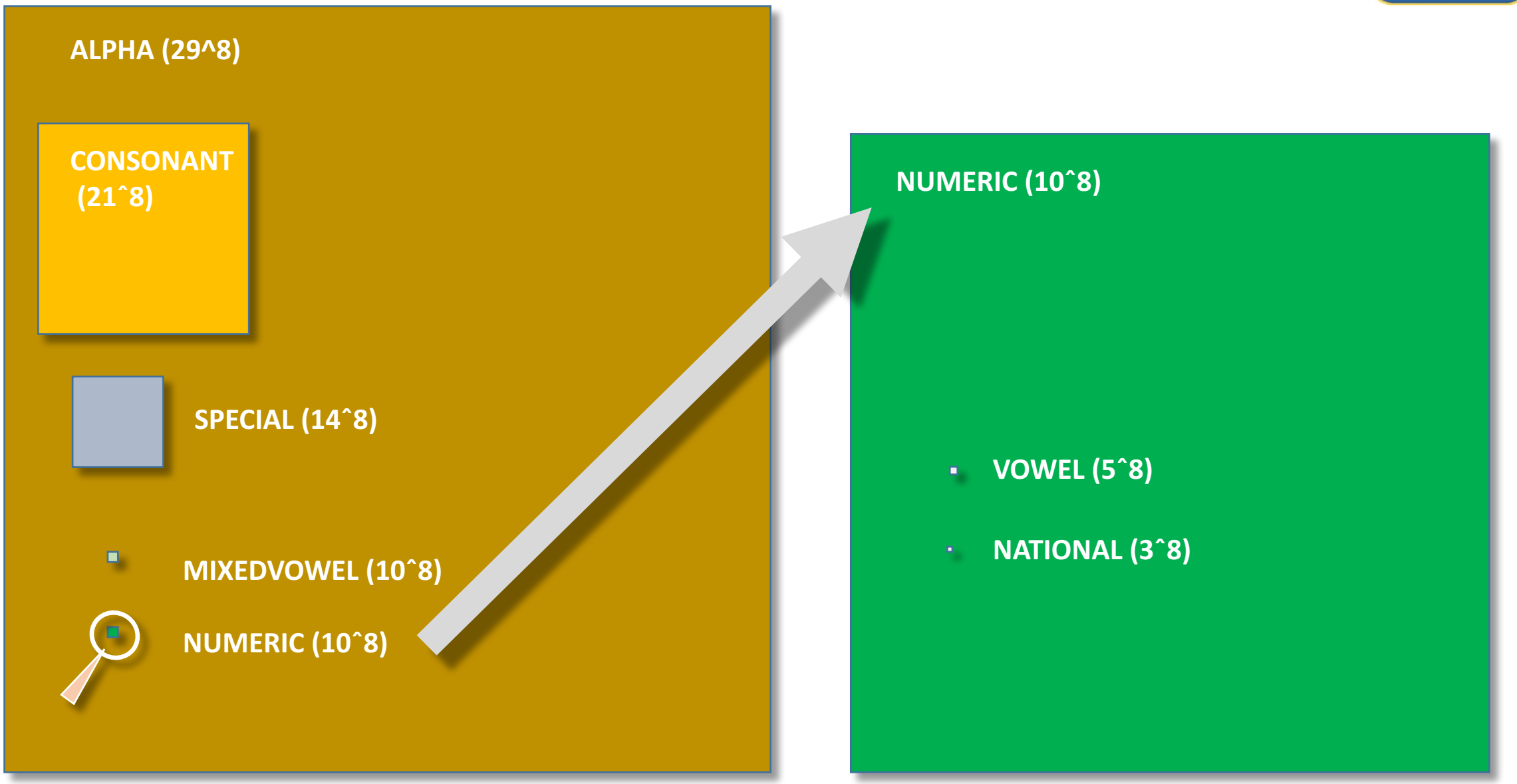
- Passwords of length 8
- Repeated symbols allowed

Each square represents the relative size of each search space. The length of the side represents the square-root of the search space.

Complex Passwords - Fact and Not Fiction – Dec 2017 Update

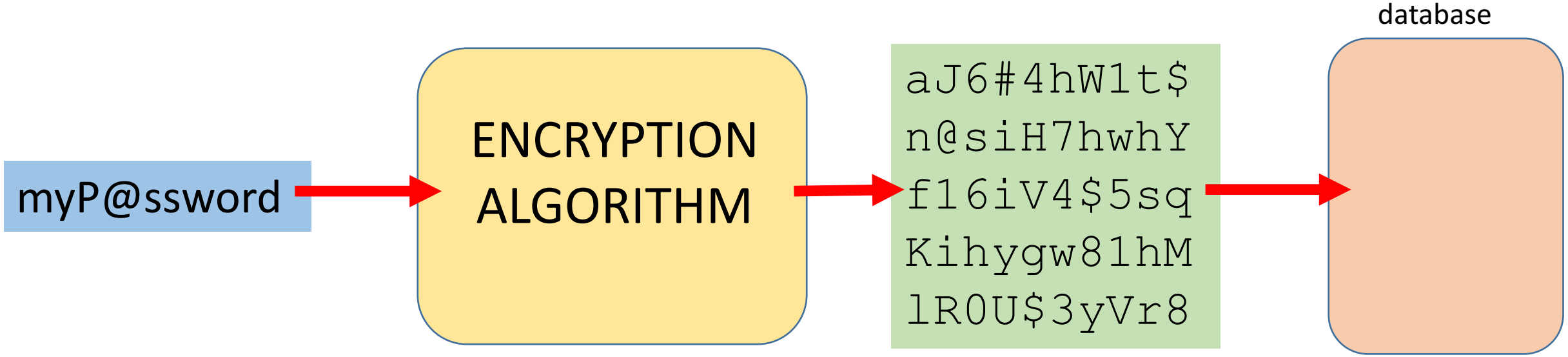


Complex Passwords - Fact and Not Fiction – Dec 2017 Update

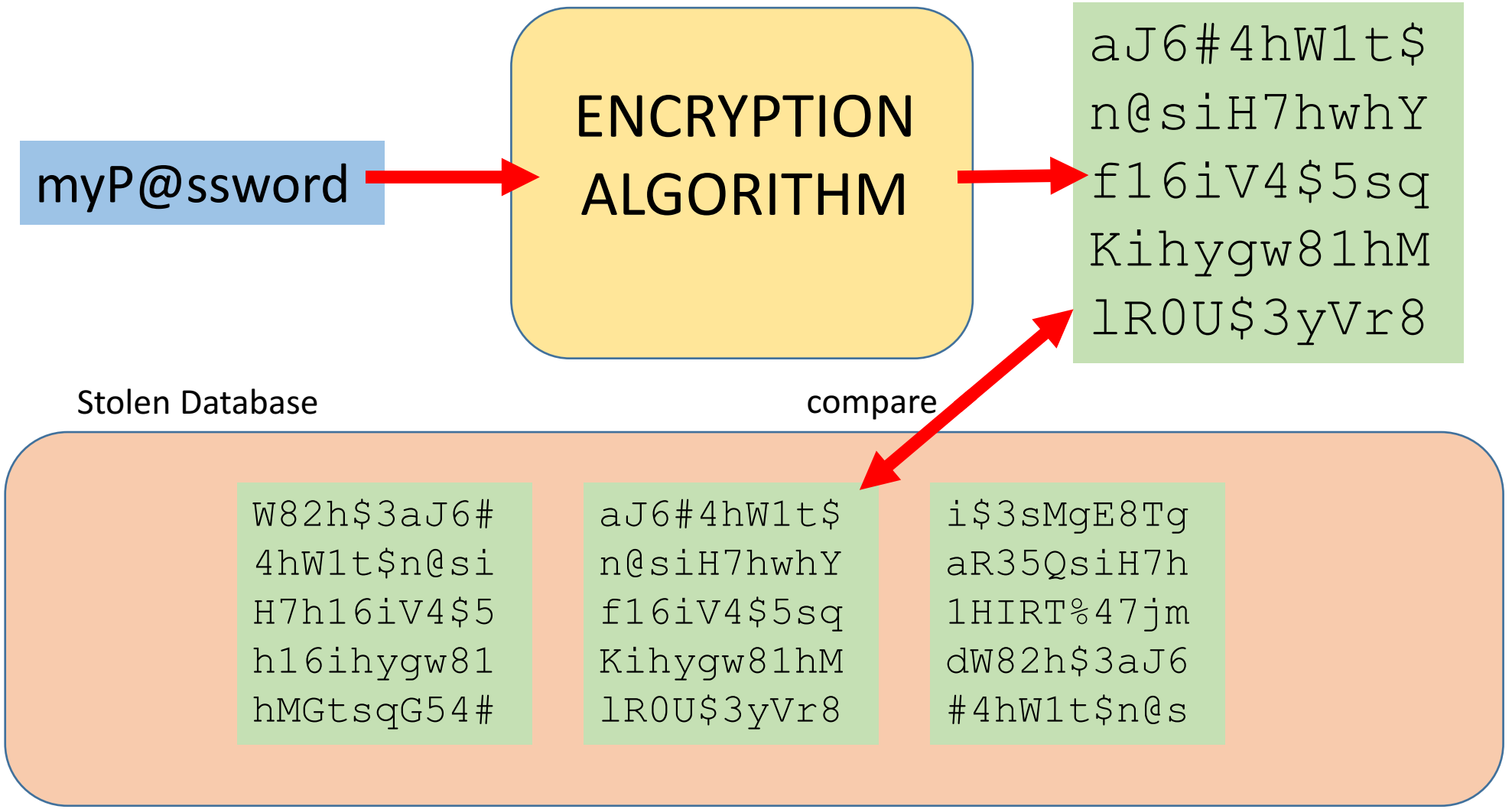


Password Mathematics: Hashing

- Passwords are not stored in the database
- Hashes are stored in the database



Password Mathematics: Hashing

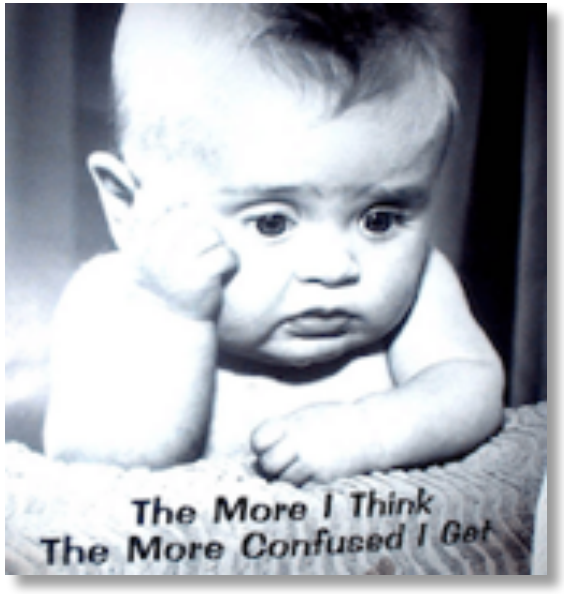


Password Mathematics: Hashing times

	A	B	C	D
21				
22				TIME TO HASH ALL POSSIBLE PASSWORDS
23				HASHES PER SECOND:
24	# SYMBOLS	# COMBINATIONS - 8 CHARS LONG	DESCRIPTION OF SYMBOLS	40,000,000
25	1	1		
26	2	256		
27	3	6,561		
28	4	65,536		
29	5	390,625		
30	6	1,679,616		
31	7	5,764,801		
32	8	16,777,216		
33	9	43,046,721		SECONDS
34	10	100,000,000	NUMERIC ONLY	2.50
35	11	214,358,881		
36	12	429,981,696		
37	13	815,730,721		
38	14	1,475,789,056		
39	15	2,562,890,625		
40	16	4,294,967,296		
41	17	6,975,757,441		
42	18	11,019,960,576		
43	19	16,983,563,041		
44	20	25,600,000,000		MINUTES
45	21	37,822,859,361	ALPHA - WITHOUT VOWELS	15.76
46	22	54,875,873,536		
47	23	78,310,985,281		
48	24	110,075,314,176		
49	25	152,587,890,625		MINUTES
50	26	208,827,064,576	ALPHA UPPER CASE	87.01
51	27	282,429,536,481		

Crafting Complex Passwords:

"…you can end up making the new password rules SO complex it can be a virtual impossibility **for a standard issue human being** to come up with a new password that fits those rules."*



* z/Auditing Essentials - VOLUME 2 – For CA ACF2 -
Julie-Ann Williams, Mark Underwood, Craig Warren http://www.newera-info.com/eBooks.html

Crafting Complex Passwords: Tools the user brings

- Professional and personal integrity.
- Intelligence – with smarts, you can be clever, too.
- A system for crafting complex passwords.

Crafting Complex Passwords: A System

- **Mnemonics vs Words**
  Can foil a dictionary or reserved word attack
  Personal: easy to remember, difficult to guess

- **Symbol substitution;**

@ for a	# for H	$ for S	5 for S	3 for E
7 for T or L	1 for i or L	8 for B	4 for A	6 for b

Symbol substitution:

- P@ssword ???
- P@55w0rdP#r@5e ???
- w!cF2LbMwMbJ0Mk YES!
- T1wBavDp2CbiHsm#as%mi
  Even BETTER!

Crafting Complex Passwords: A System

- **Rhythmic element – to further obscure the mnemonic**

  The rhythm element is imposed on the password by which keystrokes are SHIFT-ed and which are not.

  Remember the keystrokes and the rhythmic element.

Available symbols: SHIFT-able keys

Crafting Complex Passwords: A System

Sample passwords created by this method:

```
dQ6Fj@lC
DYkt#T4j
llMHi$Fc
```

Crafting Complex Passwords: Mnemonic with swap & rhythm

SOURCE: do quick brown foxes jump around lazy cats?

MNEMONIC: D Q B F J A L C

MNEMONIC: DQBFJALC **[LEVEL 1]**

SWAP: DQ**6**FJ**@**LC **[LEVEL 2]**

RHYTHM: .|.|.|.|

PASSWORD: dQ6Fj@lC **[LEVEL 3]**

(contains upper/lower case, numeric, special symbols)

Crafting Complex Passwords: Mnemonic with swap & rhythm

SOURCE: Do you know the way to San Jose

MNEMONIC: D Y K T W T S J

MNEMONIC: DYKTWTSJ **[LEVEL 1]**

SWAP: DYKT**3**T**$**J **[LEVEL 2]**

RHYTHM: ||..||..

PASSWORD: DYkt#T4j **[LEVEL 3]**

(contains upper/lower case, numeric, special symbols)

Crafting Complex Passwords: Mnemonic with swap & rhythm

SOURCE: I left my heart in San Fran cisco

MNEMONIC: I L M H I S F C

MNEMONIC: ILMHISFC **[LEVEL 1]**

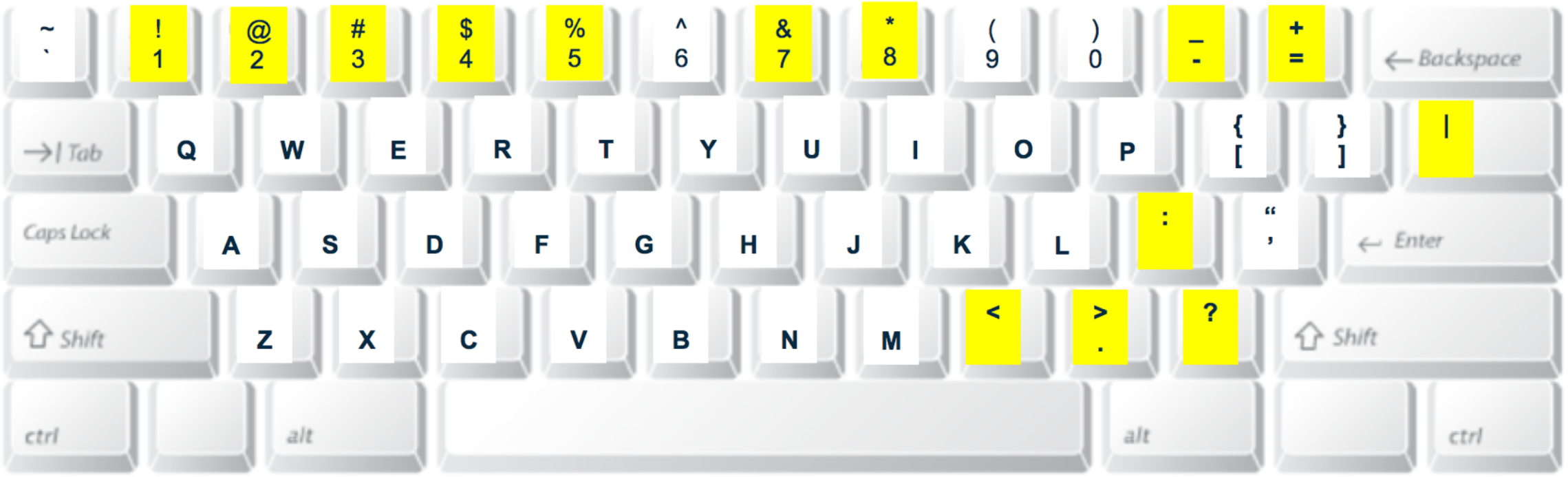
SWAP: ILMH**1$**FC **[LEVEL 2]**

RHYTHM: ..||.||.

PASSWORD: ilMH1$Fc **[LEVEL 3]**

(contains **upper/lower case, numeric, special symbols**)

Available symbols: SHIFT-able keys (RACF special symbols)



Available symbols: SHIFT-able keys (ACF2 special symbols)

NOT symbol - PC: alt + 0172 Mac: option + L ¬

Available symbols: SHIFT-able keys (TSS special symbols)

Crafting Complex Passwords: RACF – special characters

SOURCE: Great minds think alike. Not so! Be unique.

MNEMONIC: G M T A N S B U

MNEMONIC: GMTANSBU **[LEVEL 1]**

SWAP: G**3**T**@**N**5**BU **[LEVEL 2]**

RHYTHM: |.|.||..

PASSWORD: G3T2N%bu **[LEVEL 3]**

(contains upper/lower case, numeric, special symbol)

Crafting Complex Passwords: ACF2 – special characters

SOURCE: Ada Lovelace wrote programs well before their time

MNEMONIC: A L W P W B T T

MNEMONIC: ALWPWBTT **[LEVEL 1]**

SWAP: A**73**PWB**+**T **[LEVEL 2]**

RHYTHM: .|.|.|.|

PASSWORD: a&3PwB=T **[LEVEL 3]**

(contains upper/lower case, numeric, special symbols)

Crafting Complex Passwords: TSS – special characters

SOURCE: Some rabbits love carrots stolen from my garden

MNEMONIC: S R L ^ S F M G

MNEMONIC: SRL^SFMG **[LEVEL 1]**

SWAP: **5**RL^**$**F**3**G **[LEVEL 2]**

RHYTHM: .|.|.|.|

PASSWORD: 5Rl^4F3G **[LEVEL 3]**

(contains upper/lower case, numeric, special symbols)

Crafting Complex Passwords: TSS – special characters

SOURCE: Chicken cross the road? Get to other side.

MNEMONIC: C C T R G T O S

MNEMONIC: CCTRGTOS **[LEVEL 1]**

SWAP: C{TRG2OS **[LEVEL 2]**

RHYTHM: ||.||.|.

PASSWORD: C{tRG2Os **[LEVEL 3]**

(contains upper/lower case, numeric, special symbols)

Crafting Complex Password Phrases:

SOURCE: Well I come from A la ba ma with my ban jo on my knee

MNEMONIC: W I C F A L B M W M B J O M K

MNEMONIC: WICFALBMWMBJOMK **[LEVEL 1]**

SWAP: W**1**CF**@**LBMWMBJ**0**MK **[LEVEL 2]**

RHYTHM: .|.|.|.|.|.|.|.

PASSWORD: w!cF2LbMwMbJ0Mk **[LEVEL 3]**

(contains upper/lower case, numeric, special symbols)

Crafting Complex Password Phrases:

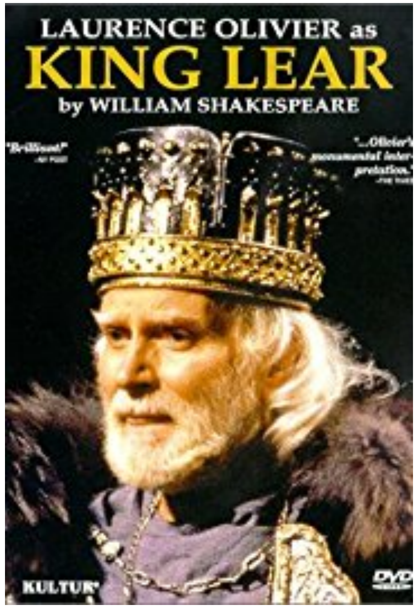
SOURCE: Attend me now, for to my head it came to tell the story of one king
MNEMONIC: A T M N F **2** M H I C **2** T T S R O **1** K

MNEMONIC: ATMNF**2**MHIC**2**TTSRO**1**K **[LEVEL 1]**

SWAP: ATMNF2MHIC2TTSRO1K **[LEVEL 2]**

RHYTHM: .|.|.|.|.|.|.|.|.|

PASSWORD: aTmNf**@**mHiC2TtsrO1K **[LEVEL 3]**



(contains upper/lower case, numeric, special symbols)

Crafting Complex Password Phrases:

SOURCE: This 1 will be a very difficult password 2 crack because it has so many hashes and some 5ymbols mixed in

MNEMONIC: T**1**WBAVDP**2**CBIHSM**#**AS**5**MI **[LEVEL 1]**

SWAP: T**1**WBAVDP**2**CBIHSM**#**AS**5**MI **[LEVEL 2]**

RHYTHM: |..|..|..|..|..|..|..

PASSWORD: T1wBavDp2CbiHsm#as%mi **[LEVEL 3]**

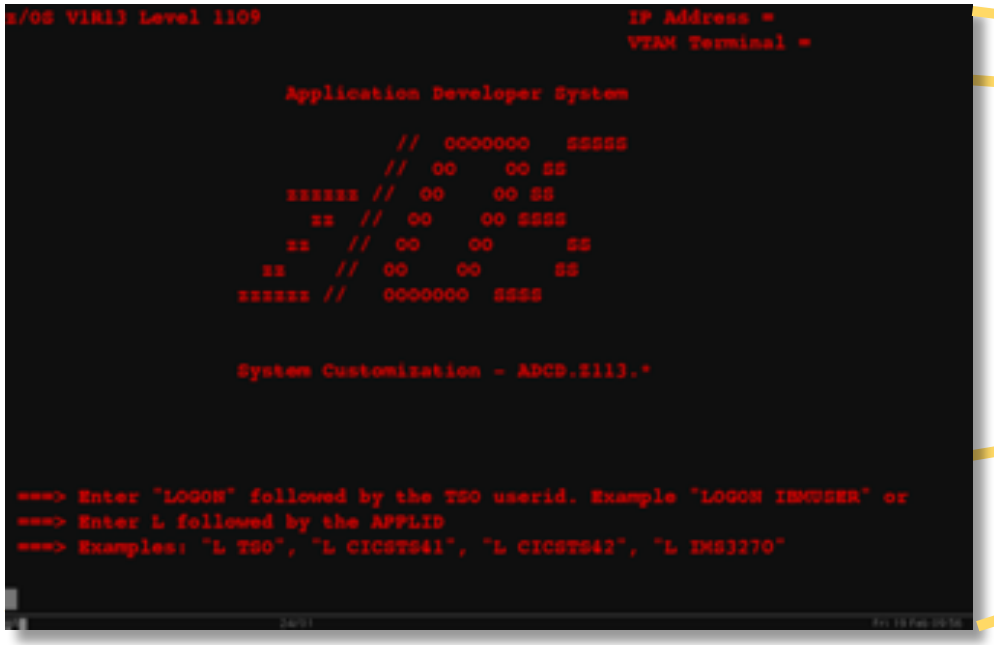
(contains upper/lower case, numeric, special symbols)

Taking it to the next step…

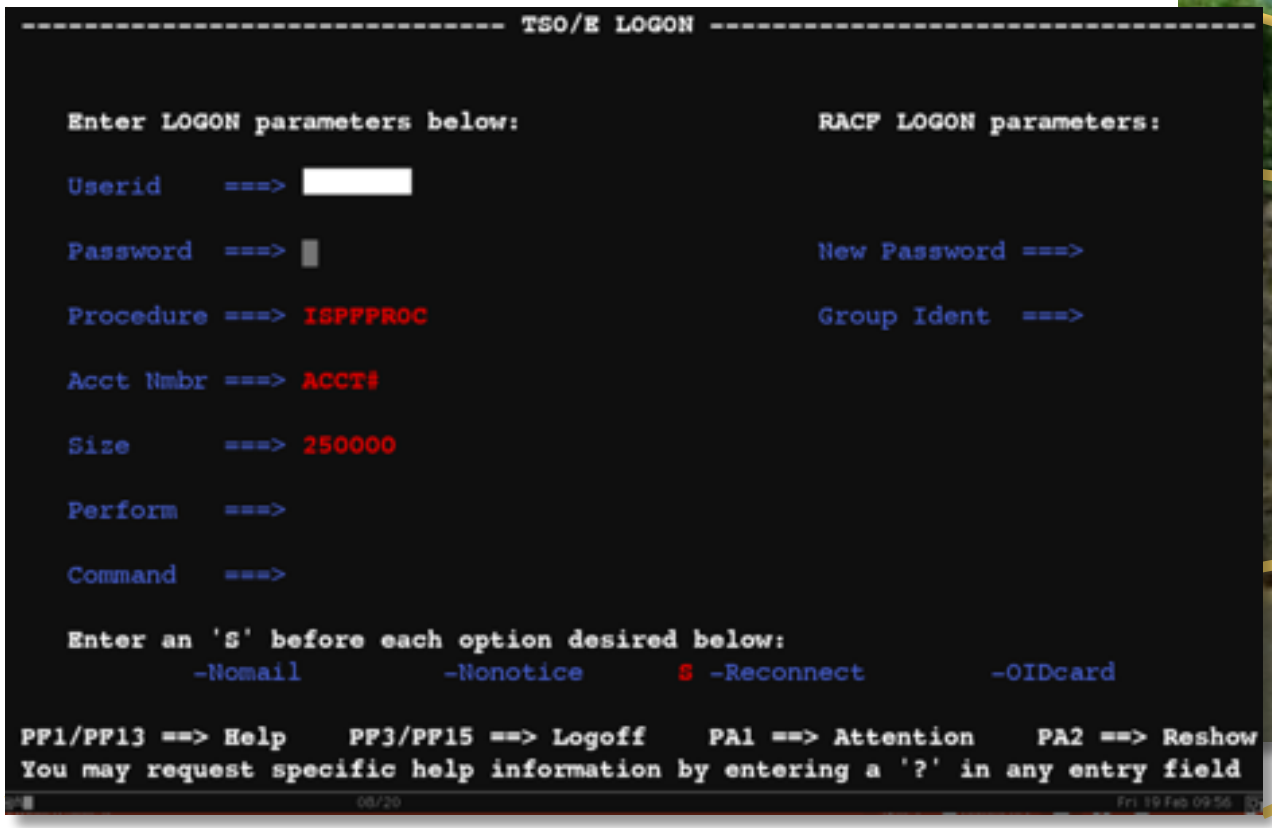
- NewEra RACF Enrichment Program
- You hold the keys to the kingdom

USERID and PASSWORD represent the KEYs to the kingdom. . .

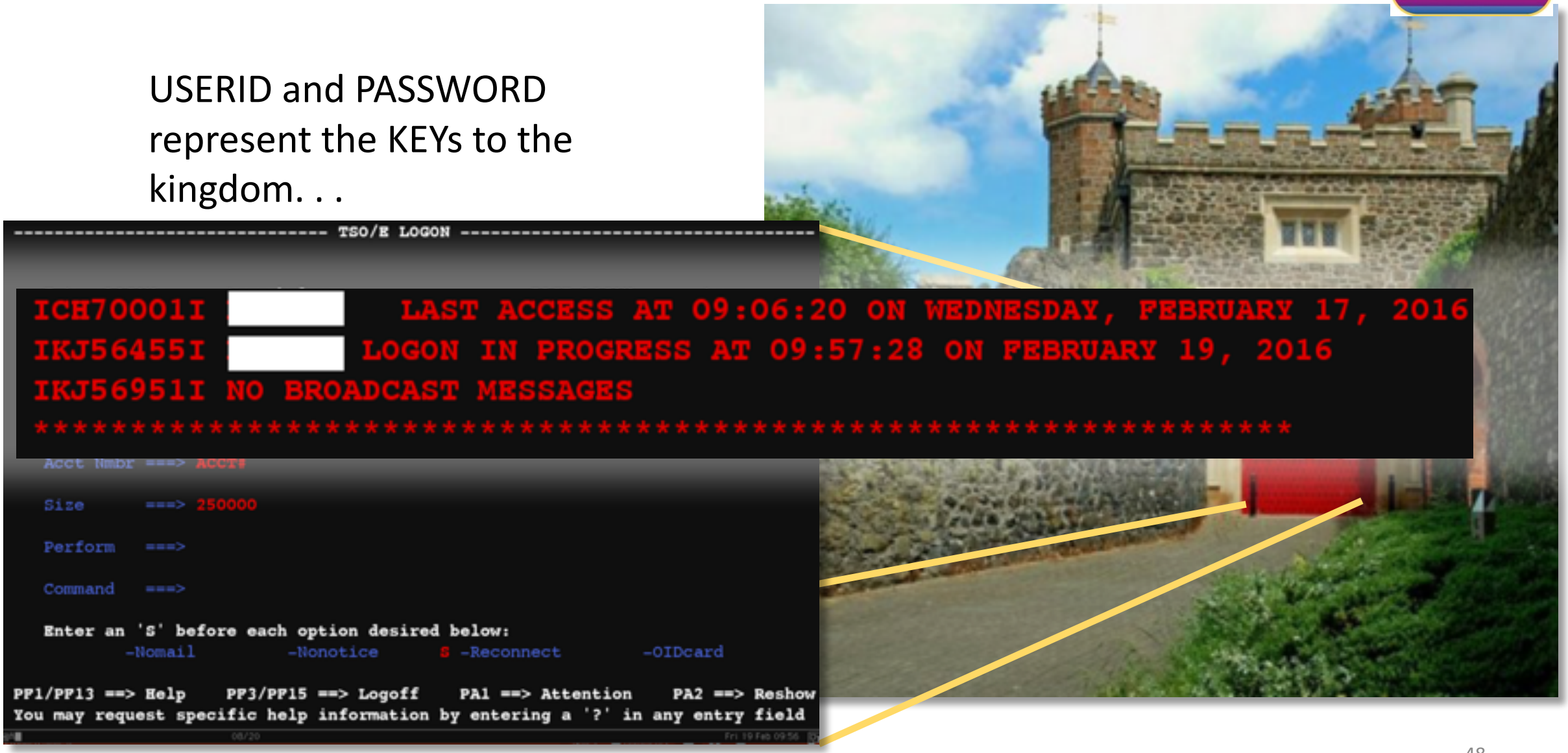
USERID and PASSWORD represent the KEYs to the kingdom. . .



USERID and PASSWORD represent the KEYs to the kingdom. . .



USERID and PASSWORD represent the KEYs to the kingdom. . .



Taking it to the next step…

- NewEra RACF Enrichment Program
- You hold the keys to the kingdom
- The only person who ACTUALLY knows what you're doing, at any point in time, is YOU!
- Getting YOU, the USER, involved in the overall system security paradigm
- Watch this space, early next year. . .

Useful and Interesting Links:

IBM Documentation on Password Phrases –

Security Server RACF - Security Administrator's Guide - V2R3 (see page 78…)
Security Server RACF System Programmer's Guide – V2R3
IBM blog detailing password phrase implementation and testing.

z Exchange Presentations –

Chad Rikansrud - RSM Partners- (see Password Cracking presentation)
- http://www.newera-info.com/CR1.html
Ross Cooper – IBM – Multi Factor Authentication - http://www.newera-info.com/RC1.html

Computerphile on YouTube –

Password Cracking – with Dr. Mike Pound - https://youtu.be/7U-RbOKanYs
How to Choose a Password (more from Dr. Mike Pound) https://youtu.be/3NjQ9b3pgIg
How Not to Store Passwords - https://youtu.be/8ZtInClXe1Q
Hashing Algorithms and Security - https://youtu.be/b4b8ktEV4Bg

Richard K. Faulhaber
rkf@newera.com twitter: @faulhaber_rk