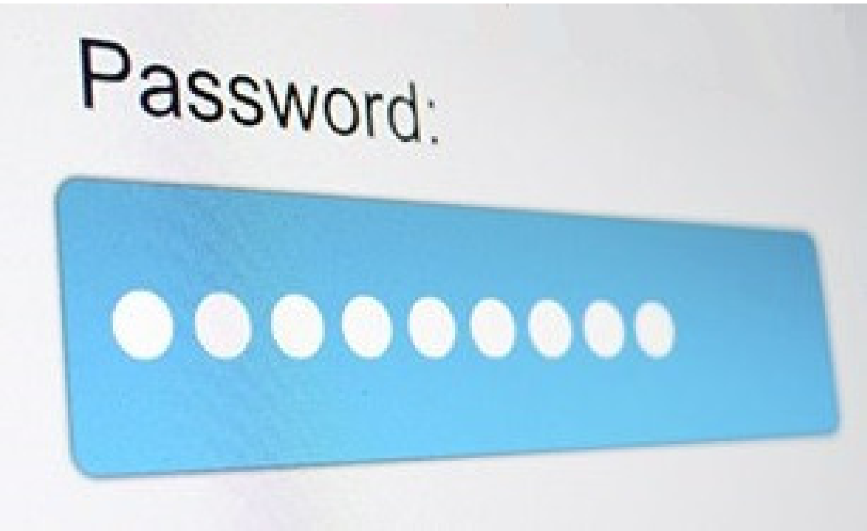
PasswordResearch.com

How Secure Are Multi–Word Random Passphrases?

Bruce K. Marshall   @PwdRsch
bkmarshall@PasswordResearch.com

Problems With Passwords

- Frequently use common words or names
- Match predictable character patterns to comply with password policies
- Too short to resist password cracking



Find the Cracked Passwords

Ohiolife12

superman

J21.redskin

Oscar+emmy2

22Jan1997

Wtamu@13

01130113monterey

thebestpasswordever

5t3ph3nl!

0racle9i

toby102

bigwaves15904

Isa15bel

%TGBbgt5$RFVvfr4

20schuyler11

Pieces10

0000194300001943

Teardrop_13

!@#$%^&*())(*&^%

nobodyhere

KRAZYkat18

blablablablablablabla

youaremysunshinemyonlysunshine

asdferfa324

$ylvester

iloveyou

V@lhall413

:LOL1313le

94UN657

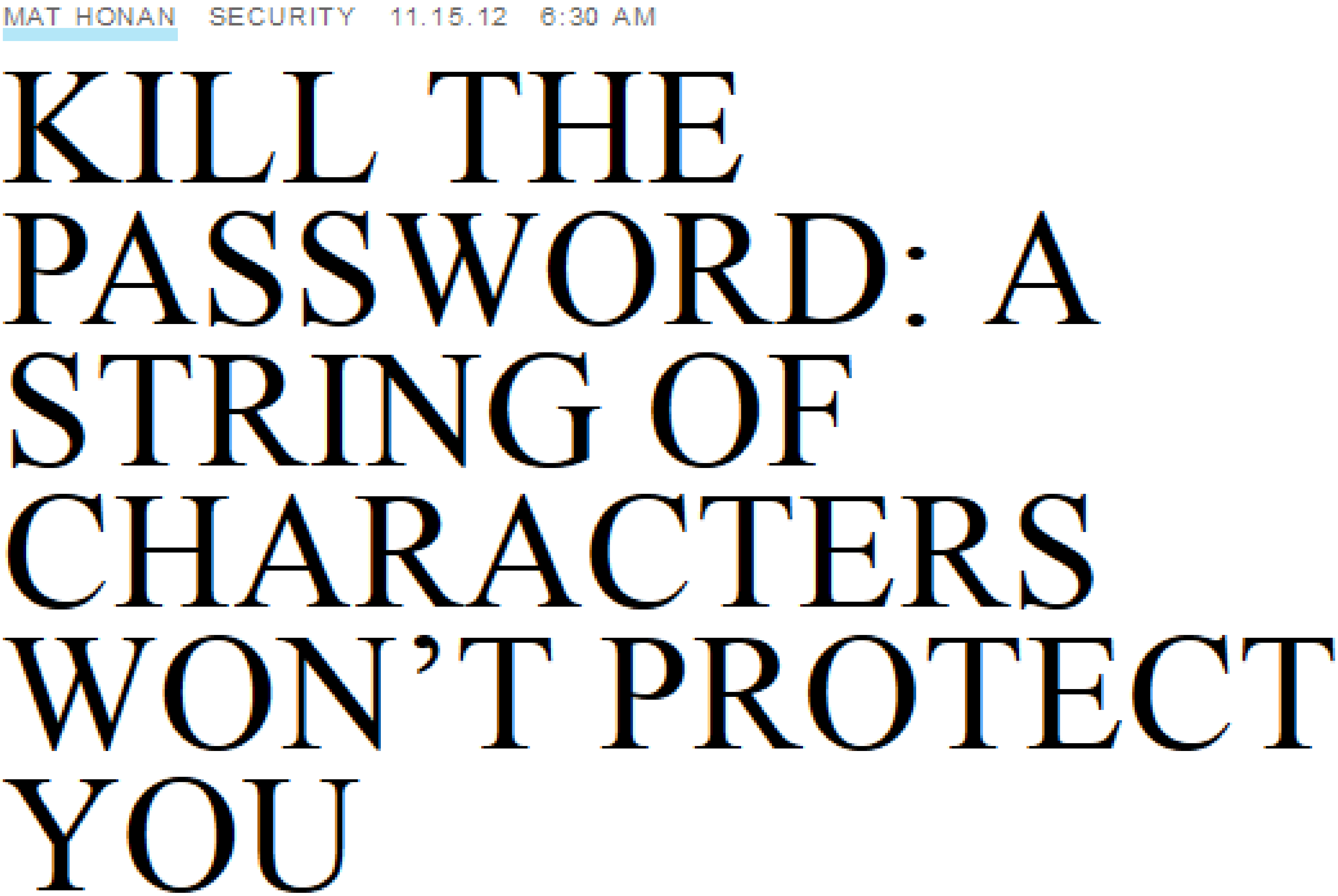
How Users Judge Passwords

- Do Users' Perceptions of Password Security Match Reality, CMU & Penn State, May 2016
  - 165 participants were shown 25 pairs of passwords and asked to identify which one was more secure

    iloveyou88 v. ieatkale88

  - Many overestimated the benefits of adding digits and using keyboard patterns
  - 67% thought their password only needed to withstand 50,000 or less guesses to be secure

[1]



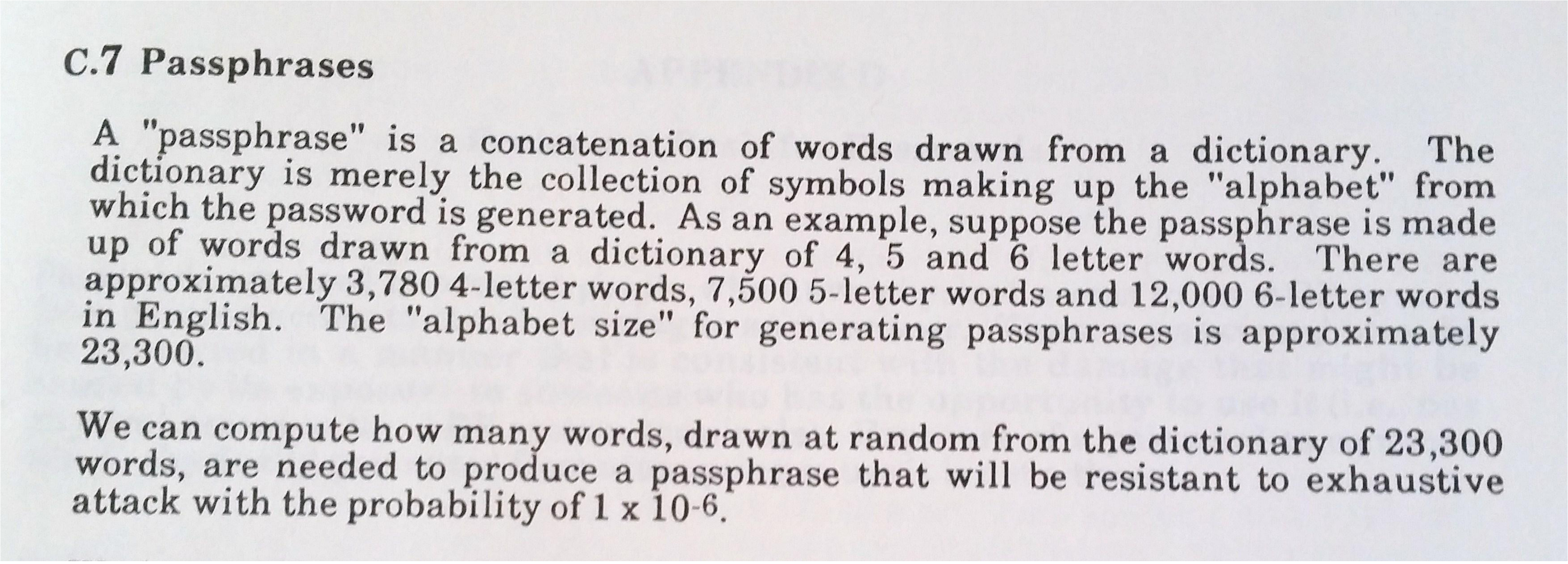
MAT HONAN SECURITY 11.15.12 6:30 AM

KILL THE PASSWORD: A STRING OF CHARACTERS WON'T PROTECT YOU

What Are Passphrases?

- Longer than passwords
- Words often separated by spaces
- Goal is to offer better security than normal passwords while also being more usable

Growing Passphrase Popularity



C.7 Passphrases

A "passphrase" is a concatenation of words drawn from a dictionary. The dictionary is merely the collection of symbols making up the "alphabet" from which the password is generated. As an example, suppose the passphrase is made up of words drawn from a dictionary of 4, 5 and 6 letter words. There are approximately 3,780 4-letter words, 7,500 5-letter words and 12,000 6-letter words in English. The "alphabet size" for generating passphrases is approximately 23,300.

We can compute how many words, drawn at random from the dictionary of 23,300 words, are needed to produce a passphrase that will be resistant to exhaustive attack with the probability of 1 x 10^{-6}.

Types of Passphrases

- Natural language phrases
  - “you can do it”
- Natural language structured random phrases
  - “fast doorway took the taco”
- Mentally selected ‘random’ words
  - “dell chair slow calendar”
- Securely selected random words
  - “land each dear spend order”

Memory Chunking

55KaDm*y? → 55 Ka Dm * y ?

chipmunk lowly stone bag spark

→

chipmunk lowly stone bag spark

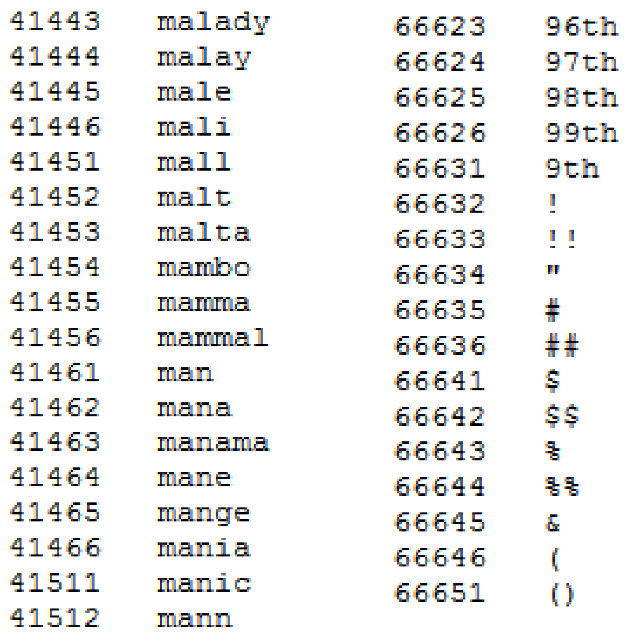
Natural Language Passphrases

- Linguistic Properties of Multi-Word Passphrases, Univ of Cambridge, 2012
  - Investigated Amazon PassPhrase, which asked customers to choose a memorable security phrase
  - Assembled word list of proper nouns, sports phrases, idioms, slang from Internet sources
  - Tested over 100,000 possible phrases, and found the best success rate with song titles, sports team names, movie titles, and superhero names
  - Concluded that user chosen passphrases were more secure than passwords, but that they still weren't sufficient against offline cracking attacks

[2]

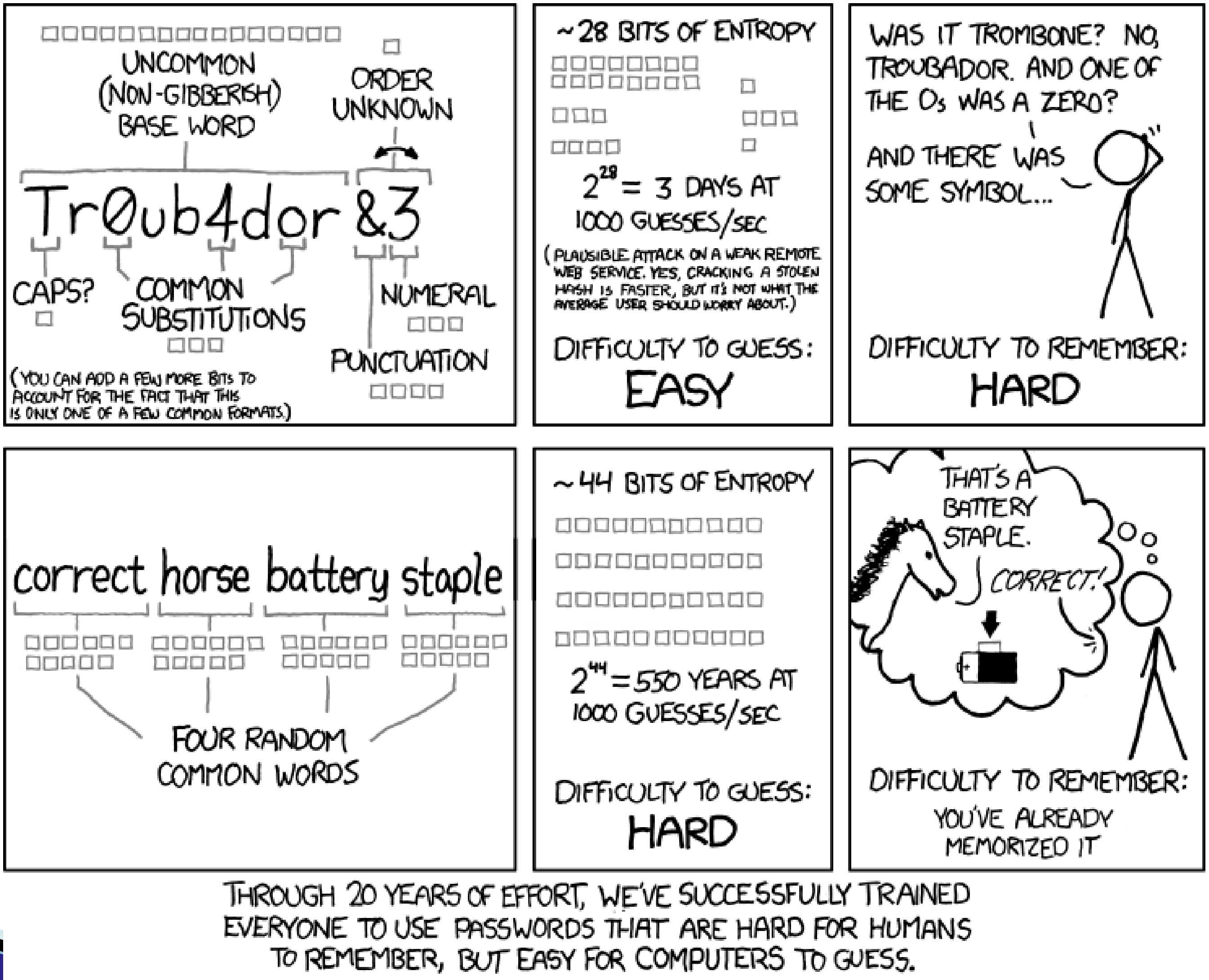
What is Diceware?

- Formal system for generating random word passphrases published in 1995 by Arnold Reinhold.
- Roll one die five times or five dice one time. Look up index of dice values and use corresponding word.



41443	malady	66623	96th
41444	malay	66624	97th
41445	male	66625	98th
41446	mali	66626	99th
41451	mall	66631	9th
41452	malt	66632	!
41453	malta	66633	!!
41454	mambo	66634	"
41455	mamma	66635	#
41456	mammal	66636	##
41461	man	66641	$
41462	mana	66642	$$
41463	manama	66643	%
41464	mane	66644	%%
41465	mange	66645	&
41466	mania	66646	(
41511	manic	66651	()
41512	mann		

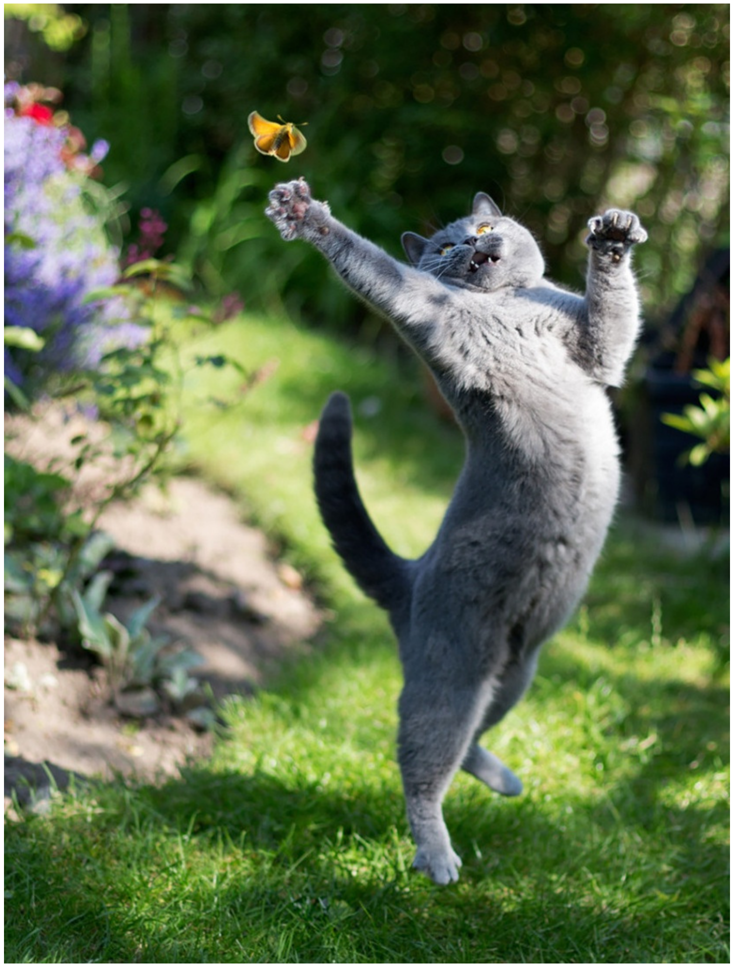
What is XKCD 936?


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^{28} = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44}=550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

By Randall Monroe, Aug 2011

Attacks Against Passphrases

- Offline Passphrase Cracking
- Online Passphrase Guessing
- Shoulder Surfing
- Keystroke Logging /
  Man-in-the-Middle /
  Phishing /
  Social Engineering /
  Rubber Hose



Resistance to Passphrases

"Don't use common words in part of your password."

"Never use dictionary words from any language as the whole or part of your password."

"Good passwords are not words in any language, slang, dialect, jargon, etc."

"A strong password should not spell a word or a series of words…"

Resistance to Passphrases

- Bruce Schneier Blog Choosing Secure Passwords, March, 2014
  - Quoted Ars Technica article from May 2013 which reported that these passwords had been cracked: “allineedislove”, “iloveyousomuch”, “sleepingwithsirens”, & “i hate hackers”

“This is why the oft-cited XKCD scheme for generating passwords – string together individual words like "correcthorsebatterystaple" – is no longer good advice. The password crackers are on to this trick.”

Estimating Random Password Strength

P = Pool of character choices
N = Number of characters combined in series

Total possible combinations = P^N

Pool of 26 lowercase alphabetic characters used in 8 character password = 26^8

Pool of 62 lowercase and uppercase alphabetic, plus numeric characters used in 9 char password = 62^9

Estimating Random Passphrase Strength

Word pool becomes your character pool while number of characters combined becomes number of words combined

P = Pool of word choices

N = Number of words combined in series

Total possible combinations = P^N

Pool of 2048 words used in an 5 word passphrase = 2048^5

Estimating Random Passphrase Strength

Bits of strength = log2(P^N)

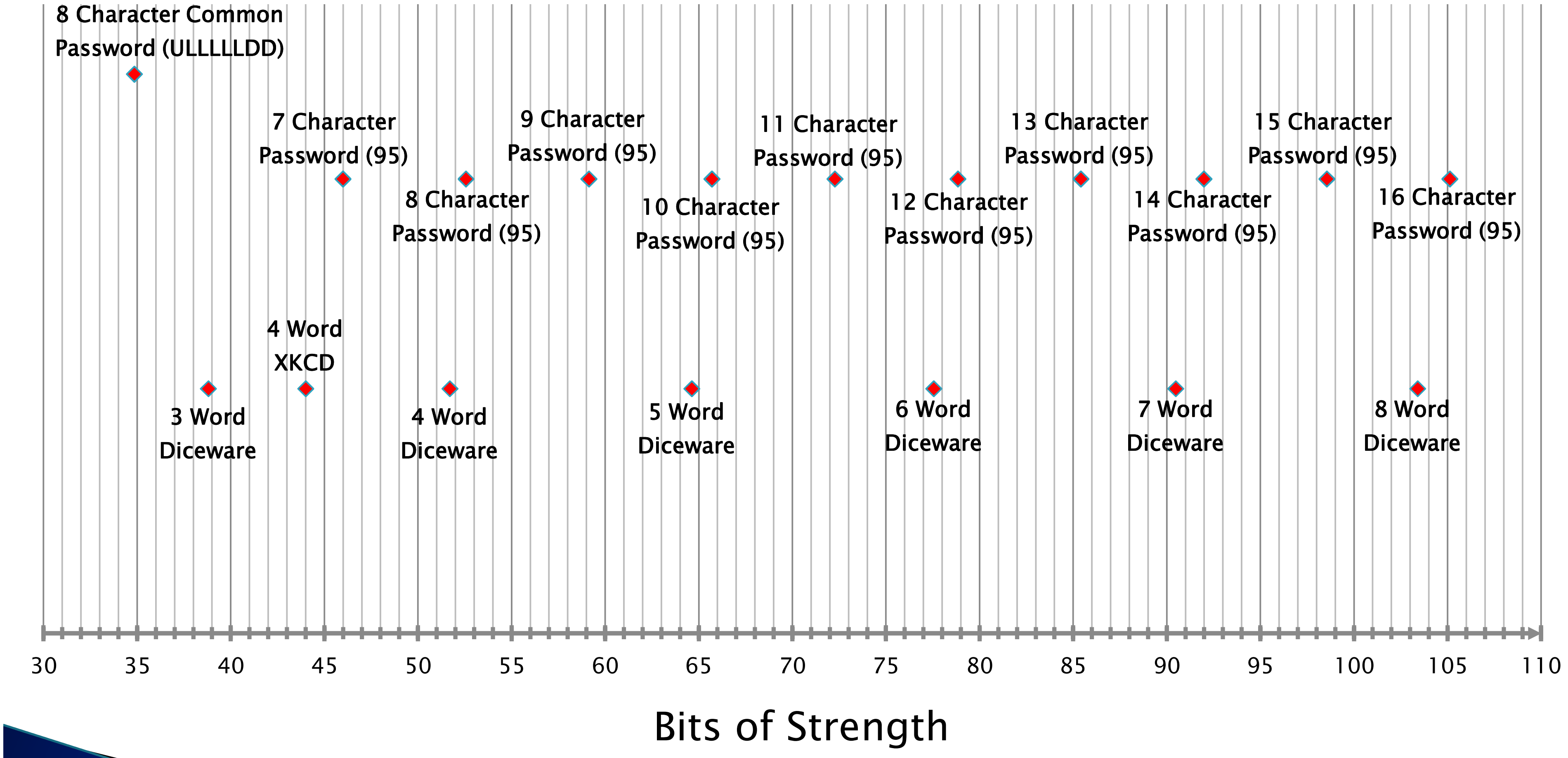
XKCD suggests using 2,048 words

2048^4 = 17,592,186,044,416 = 44 bits

Diceware has 7,776 words in base wordlist

7776^5 = 28,430,288,029,929,700,000 = 64.6 bits

How Random Passphrases Compare to Random Passwords



Concerns About Diceware Words

- Short words = chance of short passphrases
- Users face choice of using short passphrase or generating new one
- Refusing any 5 words passphrase under 14 characters eliminates 0.00037% of possible combinations

Length	Words	% of Total
1	52	0.7%
2	773	9.9%
3	839	10.8%
4	2,345	30.2%
5	3,136	40.3%
6	631	8.1%

EFF Wordlist Alternative

- Less unusual words; no vulgar words
- No numbers, special characters, or repeating letters
- Uses less short words
- Uses more longer (7-9 character) words

Length	Words	% of Total
1	0	0%
2	0	0%
3	82	1%
4	467	6%
5	928	11.9%
6	1,372	17.6%
7	1,591	20.5%
8	1,779	22.9%
9	1,557	20%

[3]

Ways to Increase Passphrase Strength

- Increase number of words combined
  - 6 words from 9,030 word list = 78.8 bits
  - Longer length can conflict with max length password policies

- Increase number of words in pool
  - 4 words from 858,000 word list = 78.8 bits
  - Larger list means less word recognition and greater possibility of recollection/entry failure

Ways to Increase Passphrase Strength

- Modify words or separator
  - Change whole word case randomly
  - Change separator from space to another symbol

CORRECT:horse:battery:STAPLE

finally+slightly+SOMETIME+UNUSUAL

silk4MANNER4ball

- 3 word Diceware = 39 bits → 47 bits
- 4 word Diceware = 52 bits → 61 bits

How Many Words to Combine?

- Diceware recommendations:
  - ~~5~~ 6 for normal use
  - 6 for wireless security / file encryption
  - 7 – 8 for 'high value' like a Bitcoin wallet
- EFF echos 6 word advice
- SecureDrop uses 7
- Shorter (e.g. 3-4 words) can still provide decent protection for lower risk apps

Cracking Passphrases

- Types of cracking attacks
- Impact of length on brute force attacks
- Kerckhoff’s principle – assume attackers know how you are creating your passwords
- Differences between password strength meter estimates and real password cracking

Passphrase Cracking Speed

	NTLM	MD5	SHA1
7-Character Password	4 minutes	6 minutes	17 minutes
8-Character Password	5.5 hours	9.2 hours	1.1 days
9-Character Password	22 days	36 days	106 days
4-Word XKCD	1 minute	1.5 minutes	4.5 minutes
5-Word Diceware	2.7 years	4.5 years	13 years
6-Word Diceware	209 centuries	350 centuries	1 K centuries
7-Word Diceware	1.6 million centuries	2.7 million centuries	7.9 million centuries

Using 8-GPU Cracker [4]

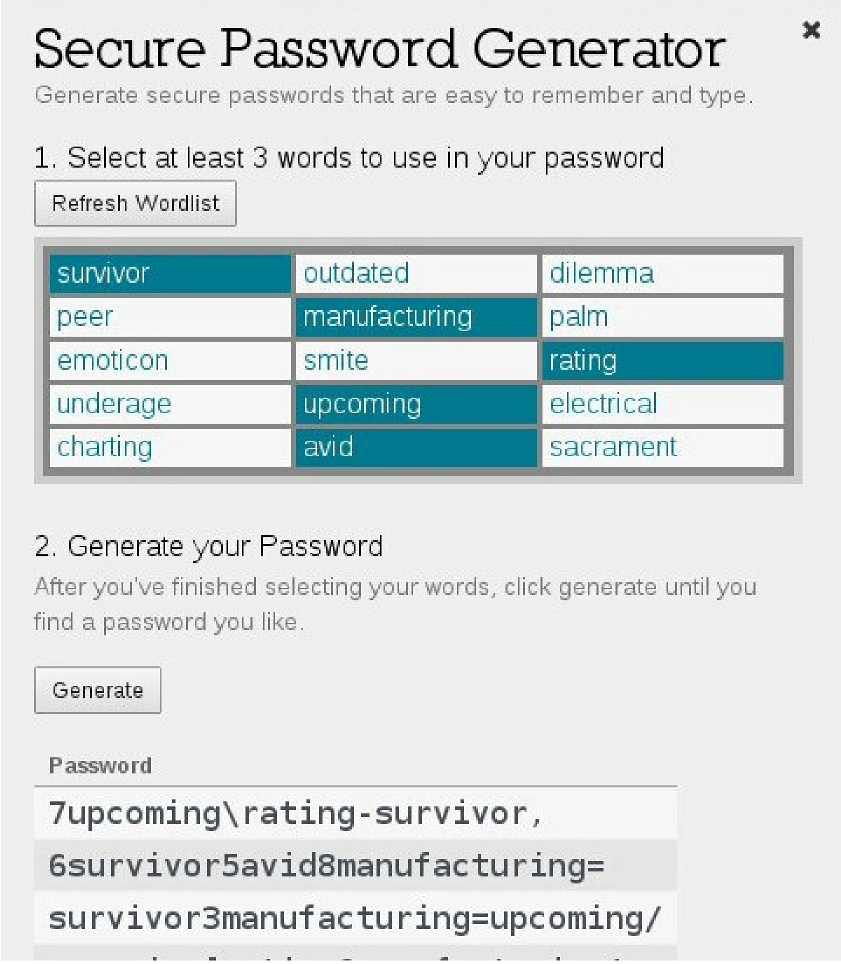
Passphrase Cracking Speed

	WinZIP PBKDF2	Bcrypt (5)	VeraCrypt PBKDF2
7-Character Password	95 days	21 years	157 years
8-Character Password	25 years	20 centuries	149 centuries
9-Character Password	24 centuries	1.9 K centuries	14 K centuries
4-Word XKCD	24 days	5.3 years	39 years
5-Word Diceware	1 K centuries	85 K centuries	637 K centuries
6-Word Diceware	8.3 million centuries	663 million centuries	4.9 billion centuries
7-Word Diceware	64 billion centuries	5.2 trillion centuries	38.5 trillion centuries

Using 8-GPU Cracker [4]

Passphrase Cracking Shortcuts

- Discover and exploit word acceptance bias
- Try natural language combinations that also match random combinations
- Collect word combos that have leaked from other sources



Secure Password Generator

Generate secure passwords that are easy to remember and type.

1. Select at least 3 words to use in your password

survivor	outdated	dilemma
peer	manufacturing	palm
emoticon	smite	rating
underage	upcoming	electrical
charting	avid	sacrament

2. Generate your Password

After you've finished selecting your words, click generate until you find a password you like.

```
Password
7upcoming\rating-survivor,
6survivor5avid8manufacturing=
survivor3manufacturing=upcoming/
```

Passphrase Usability Research

- Correct Horse Battery Staple: Exploring the Usability of System-Assisted Passphrases
  - Passphrase users took median 7 seconds to enter compared to 3 seconds for passwords.
  - No significant difference in percent of people storing passwords compared to passphrases.
  - Successful logins by passphrase non-storage participants were 47%. Compared to 58% for password. Storage groups both = 85% success.
  - The passphrases (3-4 word range) had a mean length of 18.3 / 25.5 characters.

[5]

Passphrase Usability Research

- Towards Reliable Storage of 56-bit Secrets in Human Memory, Microsoft, 2014
  - 96% of passphrase participants and 91% of random letter participants learned well enough to type from memory 3 times in a row.
  - Median typing time for all 3 segments were 8.2 seconds for words, compared to 6.1 seconds for random letters.
  - Entry errors for passphrases were median of 5 per user, with random letters a median of 7.

[6]

Passphrase Field Testing

Tested the following passphrases on large web sites & observed related usability factors:

1.	level drama whoosh funny	(24)
2.	suey 65 swim gain recur	(23)
3.	hovel strafe m's knobs lyric perm	(33)
4.	follow*RUBBER*BENEATH*natural	(29)
5.	BANAL.mayan.skit	(16)

Passphrase Field Testing – Social Media

Site	Max Length	Passphrases Accepted	Problems
Facebook	150+	All	None
Twitter	150+	All	None
Instagram	150+	All	None
Vine	100	All	None
LinkedIn	150	All	None
Pinterest	85*	All	Silently truncates

Passphrase Field Testing – Retail

Site	Max Length	Passphrases Accepted	Problems
Amazon	150+	All	None
Ebay	64	#4 & 5	Character complexity required, no spaces
AliExpress	20	None	Max length too short, no symbols allowed
Walmart	12	None	Max length too short, no spaces allowed
Target	20	#5	Max len too short, character complexity required
Ikea	20	None	Max len too short, character complexity required
Home Depot	150+	All	Some symbols cause errors

Passphrase Field Testing – Finance

Site	Max Length	Passphrases Accepted	Problems
PayPal	20	#5	Max length too short, no spaces allowed
Chase	32	#5	Max length too short, no spaces allowed
Discover	32	#2	Max len too short, character complexity required
Citigroup	50	None	Character complexity required, no spaces allowed
Wells Fargo	14	None	Max len too short, character complexity required
Bank of America	20	None	Max len too short, character complexity required, no spaces or some symbols

Passphrase Field Testing – Finance

Site	Max Length	Passphrases Accepted	Problems
Coinbase	72	All	Silently truncates
Kraken	128	#1 3 4 5	Variable complexity reqs
Simple	150+	All	None
Moven	20	#2	Max len too short, character complexity required
Mint	32	None	Max length too short, character complexity required, no spaces
Stash	72	None	Character complexity required, silently truncates
Acorns	32	None	Max length too short, character complexity req

When To Use Passphrases

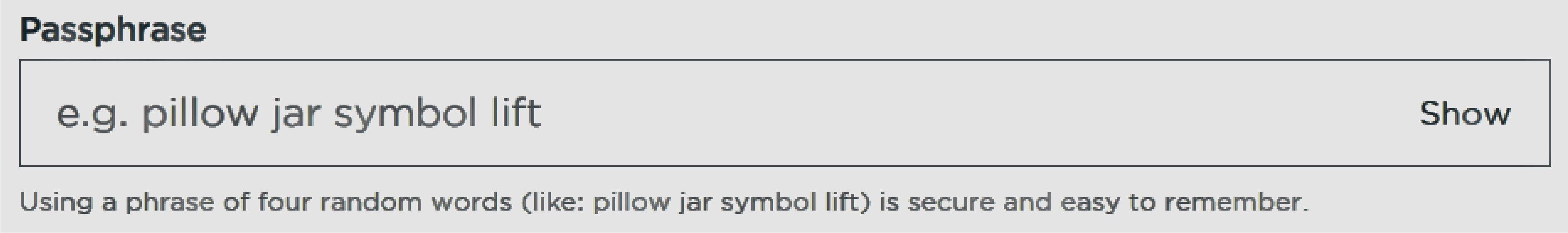
- When you have to type it regularly
- When your password manager isn’t usable or easily compatible
- When a keyboard makes them preferential versus typing random character passwords
- When you will share it with someone via voice
- For security question answers

For everything else rely on random passwords in a password manager.

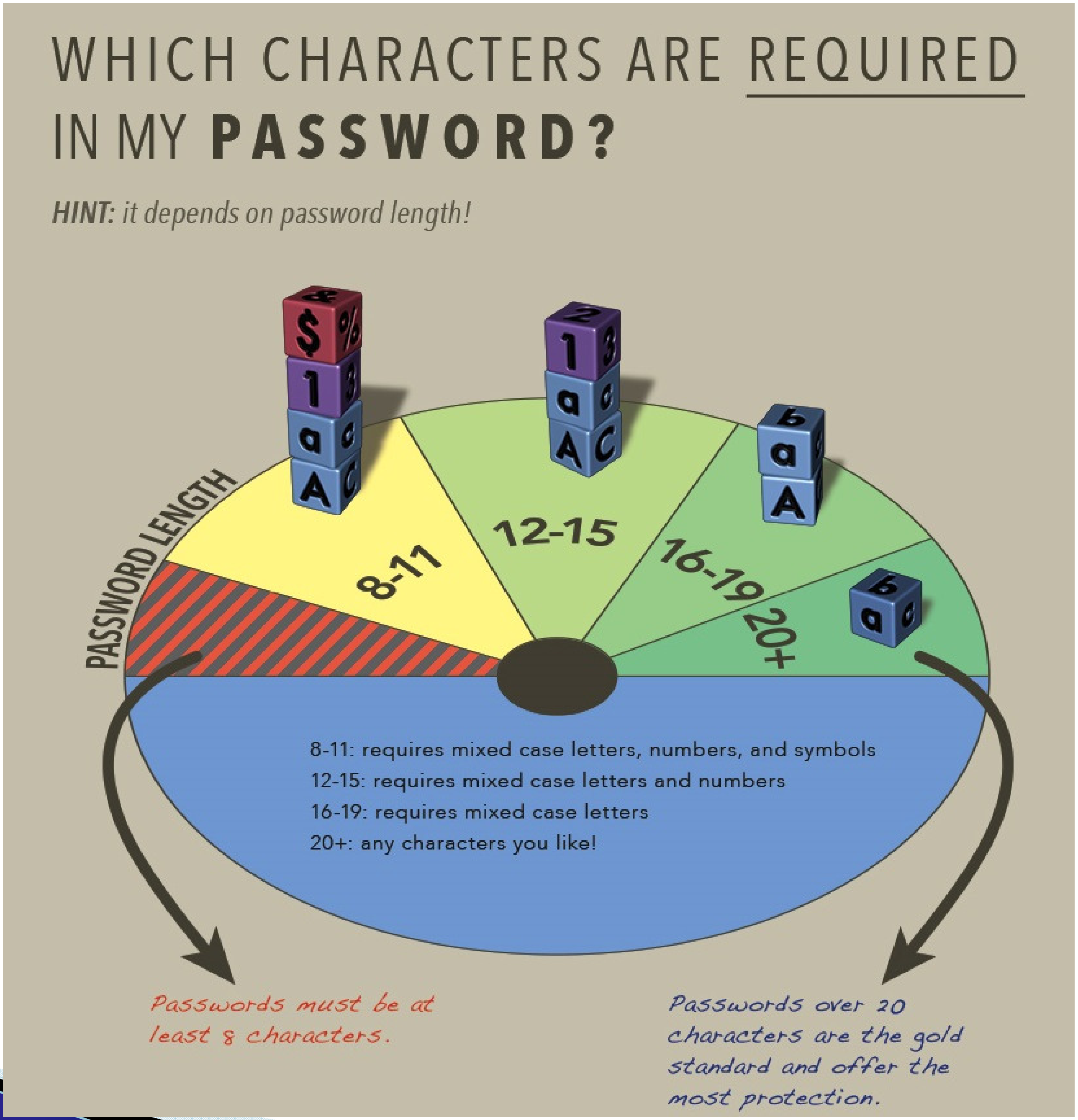
How to Support Passphrase Use

- Don’t impose unnecessary short maximum password length restrictions
- Avoid restricting symbol (and space) use
- Evaluate context of word use if preventing common dictionary words
- Provide guidance on, and examples of, good passphrase use – ideally complete systems
- Use adaptive password complexity policies

How to Support Passphrase Use



Using a phrase of four random words (like: pillow jar symbol lift) is secure and easy to remember.



WHICH CHARACTERS ARE REQUIRED IN MY PASSWORD?

HINT: it depends on password length!

8-11: requires mixed case letters, numbers, and symbols
12-15: requires mixed case letters and numbers
16-19: requires mixed case letters
20+: any characters you like!

Passwords must be at least 8 characters.

Passwords over 20 characters are the gold standard and offer the most protection.

[7]

I USE A 6 WORD PASSPHRASE
"MA MA MA MA MA MA"
Born to Rule

References

1. Do Users' Perceptions of Password Security Match Reality. Carnegie Mellon & Penn State. May 2016. http://www.blaseur.com/papers/chi16-pwperceptions.pdf
2. Linguistic Properties of Multi-Word Passphrases. Univ of Cambridge. March 2012. http://passwordresearch.com/papers/paper243.html
3. EFF's New Wordlists for Random Passphrases. July 19, 2016. https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases

References

4. 8x Nvidia GTX 1080 Hashcat Benchmarks. Jeremi Gosney, Sagitta HPC. June 2016. https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40
5. Correct Horse Battery Staple: Exploring the Usability of System-Assisted Passphrases. Carnegie Mellon Univ. July 2012. http://passwordresearch.com/papers/paper275.html
6. Towards Reliable Storage of 56-bit Secrets in Human Memory. Princeton & Microsoft. Aug 2014. http://passwordresearch.com/papers/paper374.html

References

7. Password Requirements Quick Guide. Stanford Univ. December 2015. https://uit.stanford.edu/service/accounts/passwords/quickguide

Contact Info & Slides

- Bruce K. Marshall @PwdRsch
- bkmarshall@PasswordResearch.com
- Slides available at www.PasswordResearch.com/Passphrases