Modern Times:

Passwords

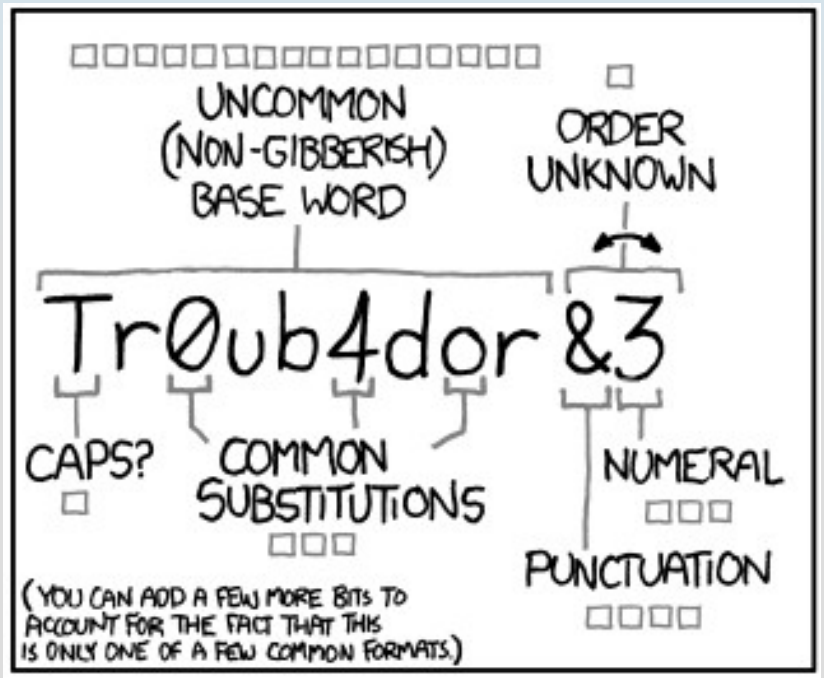
The password is old...

And we've gotten much better at breaking it over the course of human history.

The Bad Guys

- Wordlist Attacks
  - Take the most commonly-used passwords, try those first.
- Brute Force Attacks
  - Umm.. aaaaa, nope... aaaab, nope... aaaac...
- Common Account Attacks (password-reuse)
  - Is your fantasy football password the same as your company password? If the fantasy football site leaks your password, you could be in big trouble.
- Forgetting Passwords
  - Neither you, nor your helpdesk really have the time to reset passwords all day.

- Inconvenience:



The Good Guys

- Entropy (randomness)
  - Cg*Mb$bKExB&Sx06 is better than AaBbCcDdEe12345
- Length
  - It is much harder for an attacker to guess A9CKSPSA9 compared to A9CK. Longer is better.
- Rememberability
  - A password does you no good unless you can use it.
- Uniqueness
  - Don't re-use your passwords. If a service is compromised or your password is leaked somehow (think about keyloggers), you don't want everything getting compromised, only one thing. Unique passwords for everything!

The Facts

Brute Force Times (1000 guesses per second):

1234	11.11 seconds
l@Rr	22.87 hours
pass	7.92 minutes
password	6.91 years
Password	17.33 centuries
Password1	4.37 thousand centuries
PASSWORD1	33.22 centuries
P@ssword1	2.03 hundred thousand centuries
P@ssword12	19.24 million centuries

Source: https://www.grc.com/haystack.htm

Which is more secure?

Brute Force Times (1000 guesses per second):

D0g.....................	
PrXyc.N(n4k77#L!eVdAfp9	

Source: https://www.grc.com/haystack.htm

Which is more secure?

Brute Force Times (1000 guesses per second):

`D0g.....................`	93.83 billion trillion trillion centuries (24 characters)
`PrXyc.N(n4k77#L!eVdAfp9`	9.88 hundred million trillion trillion centuries (23 characters)

You don't need complexity for security.

Source: https://www.grc.com/haystack.htm

The Facts

Wordlist Attacks are designed to find and exploit commonly-used passwords and commonly used password techniques.

- How many of these do you recognize from your experience?
- How many of these have you seen people use?

Monkey01 Monkey02 Monkey03	[Common Word]+[2 Digit Sequence Number]
Password14May Password14June Password14July	[Common Word]+[2 Digit Year]+[Month]
@pple0514! @pple0614! @pple0714!	[Common Word (with common substitutions)] +[2 Digit Month]+[2 Digit Year]+[Common Punctuation]
taw201401 taw201402 taw201403	[User Initials]+[4 Digit Year]+[2 Digit Sequence Number]

The Facts

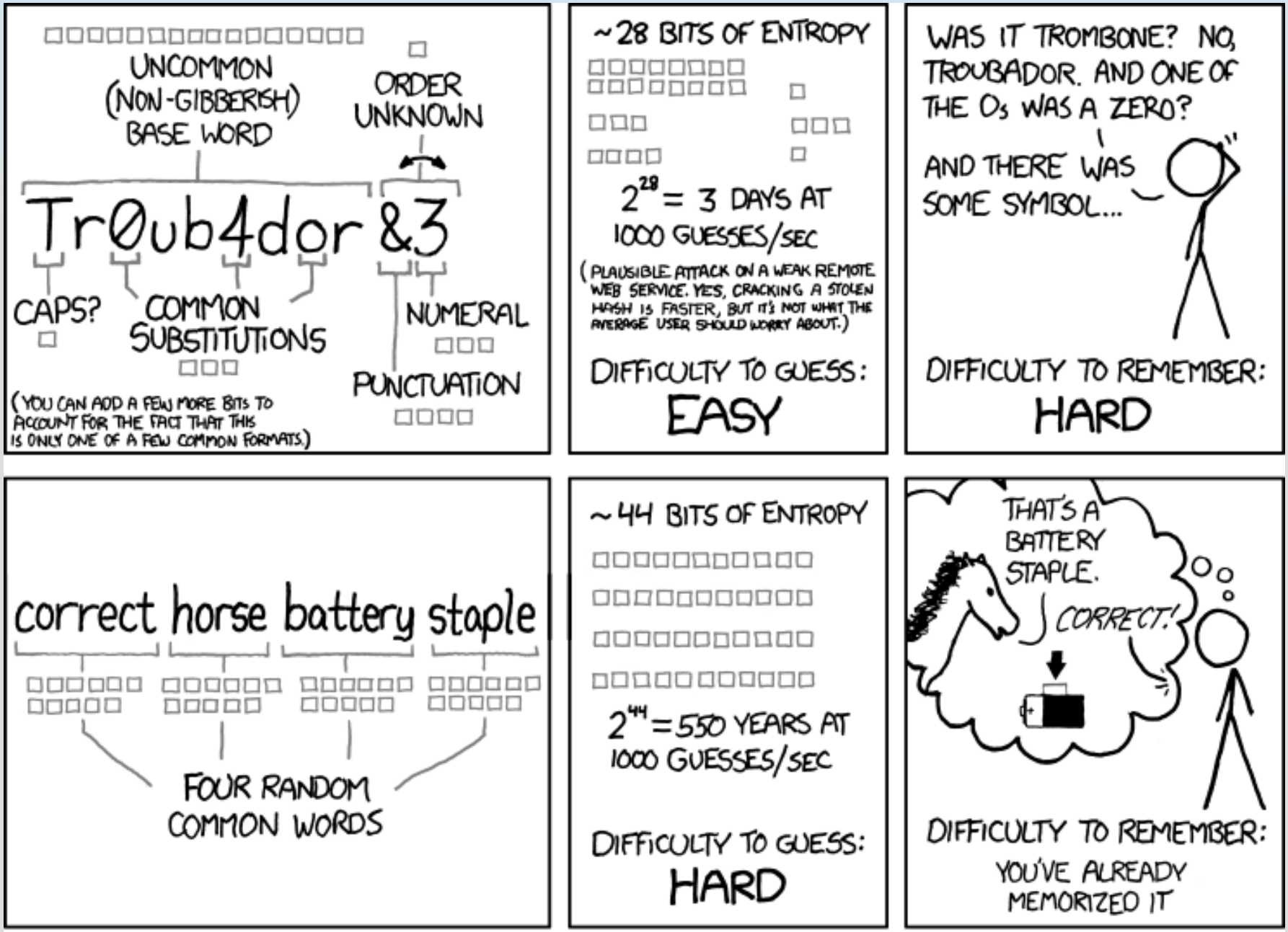
Making users change passwords regularly helps reinforce the dangerous behavior seen here.

If given an opportunity to create one really good password, people will.

Make intelligent policy decisions: Good passwords need not expire.

Monkey01 Monkey02 Monkey03	[Common Word]+[2 Digit Sequence Number]
Password14May Password14June Password14July	[Common Word]+[2 Digit Year]+[Month]
@pple0514! @pple0614! @pple0714!	[Common Word (with common substitutions)] +[2 Digit Month]+[2 Digit Year]+[Common Punctuation]
taw201401 taw201402 taw201403	[User Initials]+[4 Digit Year]+[2 Digit Sequence Number]

Correct Horse Battery Staple



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.

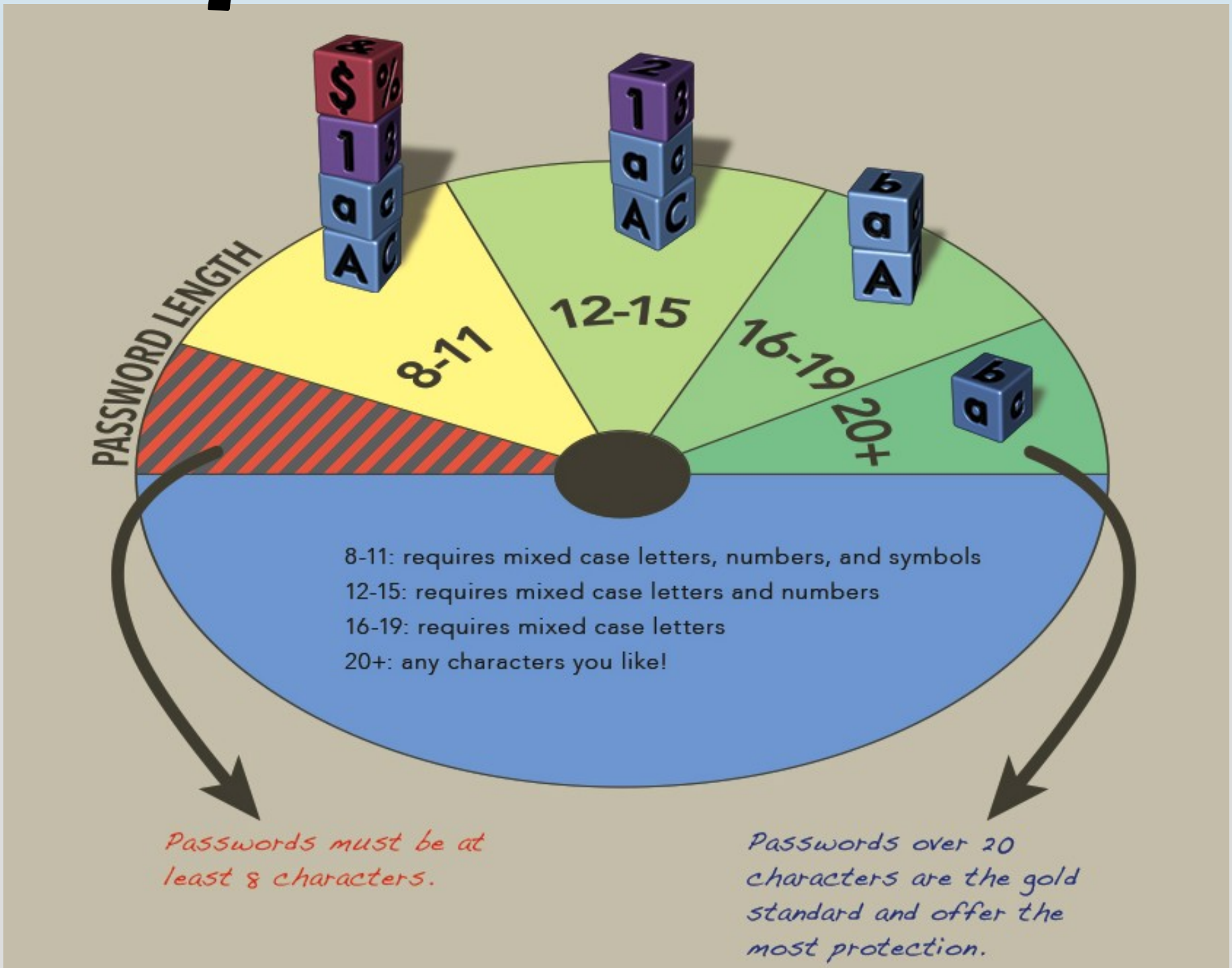
Passphrases

- Passphrases (passwords greater than 16 characters in length) are much more secure than passwords.

- Passphrases don't need the complexity that short passwords require, the length gives them enough entropy to thwart most Wordlist and Brute Force attacks.

- We should start tailoring password rules based on length (some places already do this [mostly seen in education]).

Stanford's New Rules



Recommendations

- Passphrases over Passwords
- Length over Complexity
- Wordlist Attacks will become Phraselist Attacks
  - Companies and services should adopt a list of blocked common phrases: Bible Verses, common song lyrics, etc.
- Forced password changes don't help security in any meaningful way.
  - If someone breaks in, they will run off with all of your data or infect your system with persistent malware. Changing passwords only affects silent stalkers (a very small number of password theives). Bruteforce protection is much more important and prevents users from hurting themselves.