Transactional Authentication for Data Download

Tom Winegar | Subaru Telescope | winegar@naoj.org

Sample URL:

https://ZeDvBzdRCAUr:AtoeRyYBLgiE@stars2.naoj.hawaii.edu/data/QxzjCPmZnv

(12-digit Login) : (12-digit Password) (Domain) (Download Directory)

**One download is assigned a randomized login/password –
in addition to the user's personally-selected login/password.**

Benefits: 79% average usage

a) provide an alternative to user-selected passwords
b) authenticate Co-Investigators who do not have a user account
c) prevent exposure of PI personal login/password to authenticate Co-I
d) protect against packet-sniffing for non-SSL-encryption
e) protect against command-line monitoring

Usage in NextDay Delivery vs User-Queried Transfers:

a) https: 76% NextDay vs 52% Normal = 64% average – *mainly Observers*
b) http: 98% NextDay vs 90% Normal = 94% average – *mainly Staff*

Observers choose randomized authentication ~ 2:1
Staff choose randomized authentication ~ 9:1

2013-2016
Randomized Authentication Usage

https	**65%**
http	**93%**
average	**79%**

NextDay Delivery vs Normal

	NextDay	Normal
https	**76%**	**52%**
http	**98%**	**90%**

Increase Password Security – Increase Character Set or Length?

8 character Password x 71 characters [A-Z][a-z][0-9][.%-/?@_#!]
645,753,531,245,761 = 645 trillion **71^8** → **60 days**

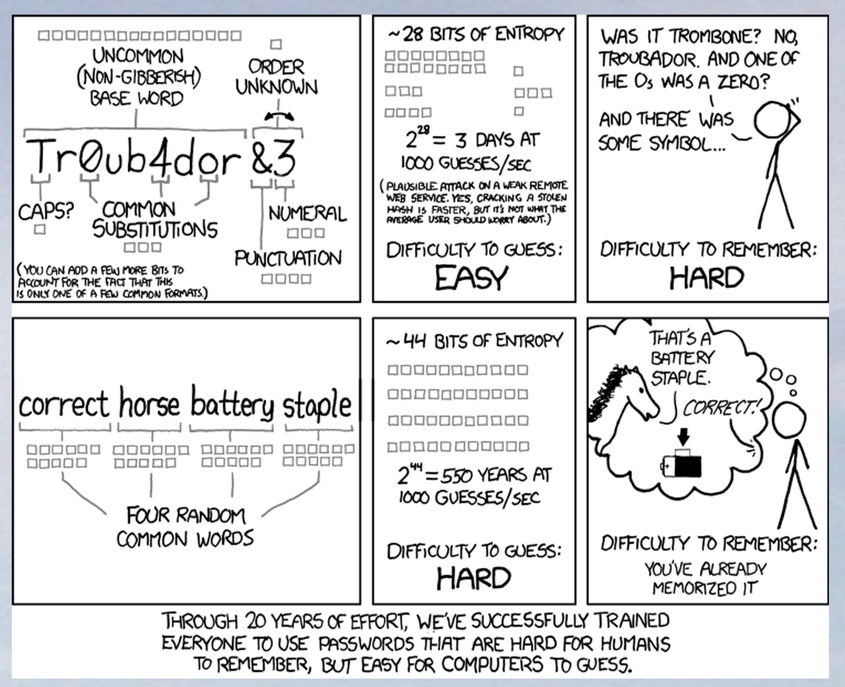
12 Character Password x 52 characters [A-Z][a-z]
390,877,006, 486,250,200,000 = 390 quintillion **52^{12}** → **62,000 years**

Brute Force Attack Estimation
1 million guesses/sec x 100 computers
@ 50% probability

Increase Password Strength – Short Passwords or Long Passphrases?

(online-domain-tools.com)

Mutable7%	**55%**	**Medium**
h@iredMic6chair	**99%**	**Excellent**



Passphrase Creation – Diceware

Randomly-select small words to construct a passphrase
5 rolls of 1 dice chooses 1 word from 7776 unique words,
concatenate passphrase of 4-6 words, use divider characters.
For more security, increase the number of words.

clawmaidbeaten4smug 99% Excellent

Word List

16655 clause	21113 cliff
16656 claw	21114 climb
16661 clay	21115 clime
16662 clean	21116 cling
16663 clear	21121 clink
16664 cleat	21122 clint
16665 cleft	21123 clio
16666 clerk	21124 clip
21111 cliche	21125 clive
21112 click	21126 cloak