Report

161325 – Prashsay Ashok | 161328 – Aman Srivastav | 161332 – Varun Saxena

A report on how to create a good password which can’t be easily guessed and characterization of password on the basis of different platforms.

Password Length vs. Password Complexity

Length is simply how much characters a person utilize in making their passwords. It plays a major role in making good passwords because the lengthier the password is, the more time an attack will need to hack into the account. So is a long password the way to go? Possibly. Lengthy passwords are often associated with an increase in password entropy, which basically is the measure of how much uncertainty there is in a key. **Password strength is directly proportional to increase in entropy.** Therefore, a lengthy list of easy-to-remember words or a passphrase could be actually more secure than a shorter list of random characters. **But if the password is not complex enough then it can be hacked easily.**

Example: "Rajeshismybestfriend" – A password with 20 characters but almost no complexity.

Complexity is often seen as an important aspect of a secure password. It is a random combination of alphanumerical characters and symbols and is intuitively seems as the best defense against cracking. **Dictionary attacks carried out won't be able to "guess" such passwords in a timely way**. But are they really effective against all attacks? Probably not. As complex passwords often tend to be shorter therefore, they are cracked in no time.

Example: "$2a4A" – A complex password but with very short length.

Combining Length and Complexity

It is now clear that length and complexity on their own are not enough. Therefore, in order to create a secure password one must combine these two factors and create a password which is **COMPLEX** as well as **LENGTHY**.

For Example: "@RaHul12*4" – A password with 10 characters which is also hard to guess due to high complexity.

A study of passwords with 8 characters

No. of Uppercase letters – 26 (A – Z)
No. of Lowercase letters – 26 (a – z)
No. of Numerals – 10 (0 - 9)
No. of Symbols – 33 (!, @, $...)

Total printable characters = 95

Total no. of possible combination = 95^8

Password with at least one of the following: (lower case letters, upper case letters, digits, punctuations, special characters).

Starting with all 8-character strings: 95^8

Then removing all passwords with no lowercase (69^8), all passwords with no uppercase (69^8), all passwords with no digit (85^8) and all passwords with no special character (62^8).

But then we removed some passwords twice. So we must add back all passwords with:

- no lowercase AND no uppercase: 43^8
- no lowercase AND no digit: 59^8
- no lowercase AND no special: 36^8
- no uppercase AND no digit: 59^8
- no uppercase AND no special: 36^8
- no digit AND no special: 52^8

But then we have added back a few passwords too many times. For instance, an all-digit password was remove three times in the first step, then put back three times in the second step, so it must be removed again:

- only lowercase: 26^8
- only uppercase: 26^8
- only digits: 10^8
- only special: 33^8

Grand total: $95^8 - 69^8 - 69^8 - 85^8 - 62^8 + 43^8 + 59^8 + 36^8 + 59^8 + 36^8 + 52^8 - 26^8 - 26^8 - 10^8 - 33^8 = 3025989069143040 \approx 3.026 \times 10^{15}$

What not to include in password!

- Your name in any form -- first, middle, last, maiden, spelled backwards, nickname or initials.
- Any ID number or User ID in any form, even spelled backwards.
- Any common name, e.g., Sue, Joe.
- The name of a close relative, friend, or pet.
- Your phone or office number, address, birthday, or anniversary.
- Any all-numeral passwords, e.g., your license-plate number, social-security number.
- Names from popular culture, e.g., HarryPotter, Sleepy.
- A single word either preceded or followed by a digit, a punctuation mark, up arrow, or space.
- Words or phrases with all the vowels or white spaces deleted.
- Words or phrases that do not mix upper and lower case, or do not mix letters or numbers, or do not mix letters and punctuation.

Why do we need complex password?

While guessing password, most password crackers have rules that can try millions of word variants per second, so the more algorithmically complex your password, the better.

Character Sets used in Password	**Calculation**	**Possible Combinations**
Dictionary words (in English): (It is debatable but let's generously say ~600,000 words)	---	600,000
Numbers Only	10^8	100,000,000
Lowercase Alpha Set only	26^8	208,827,064,576
Full Alpha Set	52^8	53,459,728,531,456
Full Alpha + Number Set	62^8	218,340,105,584,896
Full Set of allowed printable characters set	$(10+26+26+33)^8$	6,634,,204,312,890,625

The longer our password the more secure. If we take the full set of allowed printable characters set and increase the password length, the possible combinations jump exponentially.

- 8 Characters > 6, 634, 204, 312, 890, 625 (6.63 Quadrillion) Combinations.
- 9 Characters > $6.302494097246094 \times 10^{17}$ (630.2 Quadrillion) Combinations.
- 10 Characters > $5.987369392383789 \times 10^{19}$ (59.8 Quintillion) Combinations.

Characterization of Password

For Social Networking Platforms – Uppercase and lowercase letters and Numerals.

Total possible combination with 8 characters = $(26+26+10)^8 = 62^8$

For platform that uses Bank Account Information – All 95 printable characters.

Total possible combinations with 8 characters = 95^8

For ATMs – Only Numerals.

Total possible combination with 5 characters = 10^5

Note: Security can further be increased by adding –

1. Mobile Number Verification.
2. Aadhar Card Verification.
3. Additional Picture Password.
4. Additional Pin Password.