Complexity considerations for password recovery

Herve Jean-Baptiste, Wilyn St. Armand, and James Haralambides, PhD
Barry University, Miami Shores, Fl.

Password complexity is a crucial aspect of digital security. A strong and complex password can prevent unauthorized access to sensitive information, while a weak password can easily be guessed or hacked. Therefore, it is essential to understand the elements that make up a complex password. A complex password consists of a combination of upper and lowercase letters, digits, and symbols. The longer the password, the more secure it is, as it takes longer for an attacker to crack it using a brute force method. Passwords that are easy to guess, such as "password" or "123456," should be avoided, as well as those that contain personal information, such as birth dates or names. Password complexity may be further enhanced using multifactor authentication (MFA), which requires additional forms of identification beyond the password itself. The complexity of passwords is calculated using a wide range of word lengths and character sets. Permutations with duplications are used to determine the possible order or arrangement of password characters. The formula is as follows, $\sum_{r=1}^{n} P_{n,r} =$ n!$/(n-r)$!, where n refers to what is usable, and r refers to what is used. The resulting asymptotic complexity is $O(n^{r+1})$. Character sets examined include alphabetic letters, alphanumeric characters, and finally all printable ASCII characters. Data shows that the complexity of a password increased as the number of choices increased. The results suggested, for instance, the difference between an 8-character password made up entirely of lowercase letters and one made up of alpha-numeric characters and symbols is a 99.998714715734% difference.