Password Proximity Algorithm

Jeng, Yu-Shiang

Password security has become an increasingly high priority nowadays as more and more information is becoming stored online. This project seeks to develop a password algorithm that can quickly recognize brute force password generators as well as boost efficiency for the user (by providing accountability for typos). The algorithm has been designed to compare the user's entered password with the user's stored password and generate a value based on letter proximity. The value of proximity can then be used to reflect the number of password attempts allotted to the user. Both security and efficiency can be achieved through such an algorithm. Brute force bots would be quickly barred from entering a password, since the attempts entered by the intruder would be likely be wildly different from the stored password. This would result in a high string proximity and a lower number of remaining attempts. On the other hand, if the user makes a small typo, the string proximity would be low, which would translate into a larger number of remaining attempts. The security or “hackability” of the password proximity algorithm (PPA) has been calculated by a separate program called PPA_Verifier_Length. These findings report that hackers have a significantly lower success rate on programs using password proximity versus programs not using password proximity.