Better passwords get with the beat

17 May 2011

No password is 100% secure. There are always ways and means for those with malicious intent to hack, crack or socially engineer access to a password. Indeed, there are more and more websites and databases compromised on a seemingly daily basis. A new approach to verifying passwords that also takes into account the speed with which a user types in their login and the gaps between characters would render a stolen password useless.

Writing in the *International Journal of* Internet Technology *and Secured Transactions* computer scientists from Beirut explain the shortcomings of previous attempts at key-pattern analysis. KPA is an attempt to scrutinize the speed with which a user taps the keys as well as measuring the gaps between keystrokes, the beat of their typing. KPA has also been tested with modified keyboards that measure the force with which keys are pressed. The result can be a biometric profile of the way an individual user types in their password. If the biometric does not match the user then the password fails even if it is "correct".

Ravel Jabbour, Wes Masri and Ali El-Hajj of the American University of Beirut, in Lebanon, point out how inconvenient a modified keyboard would be to an organization or individual. They explain how previous attempts at KPA fail if the pressing of two keys overlaps. Early efforts also focus on "inter" timing, the time lag between pressing one key and the next, which is not adequate to ensure a password is usable only by the legitimate user. The team instead has incorporated "intra" timing that measures how long each key remains depressed, which they say gives them the beat of the typing and is a much more robust parameter.

The program gathers information about how the user is typing in their password by recording the electronic signals from a standard keyboard as keys are pressed and released. The program then compares the pattern of the password typed with a pre-stored pattern recorded when the account is initially setup. A user would be expected to repeatedly type their password at the login registration stage to record a reproducible typing pattern. The validation algorithm then looks at the various parameters, intra and inter timing the relationships between two keys (digraph), three keys (trigraph) and up to the number of keys that are the password length.

Obviously, a longer password will provide a more complicated profile of the person's typing and so reduce the risk of the typing of anyone else typing the password with the same timing pattern as the legitimate user. There is a trade-off, of course, too long a password and even a legitimate user is unlikely to reproduced their typing pattern accurately every time they enter the password. Password distribution can also be accommodated for by creating KPA groups for the same password for those users eager to share their passwords with friends and colleagues without impinging on the security of the system, the team says.

More information: "Optimising password security through key-pattern analysis" in *Int. J. Internet Technology and Secured Transactions*, 2011, 3, 178-193

Provided by Inderscience Publishers

APA citation: Better passwords get with the beat (2011, May 17) retrieved 16 January 2021 from https://phys.org/news/2011-05-passwords.html