# Can typing habits prevent cybercrime?

September 11 2015

New research published in *Journal of Applied Security Research* proposes a new keystroke algorithm which intends on making online authentication processes more secure, reliable, and cheap. The new method hopes to alleviate some of the common issues for internet users including loss of password, growing prowess of hackers, and easy access to methods such as phishing and usage of bots.

Like fingerprint scans, retina scans, and facial recognition, keystroke dynamics are a biometric—they measure a unique human characteristic. "As the typing pattern varies from person to person, this can be used as a suitable method for the authentication process more effective than others," wrote the researchers. "The information needed for the process is using the various software systems already present in the computer, leading to a decrease in costs."

The new keystroke template algorithm combines measures from existing models to increase precision. To test their algorithm, the researchers built a program that users could log into using passwords of varying length. While entering their credentials, keystroke dynamics were recorded. Results indicate that their algorithm was successful in decreasing login errors and making improper authentication very unlikely, thus advancing keystroke dynamics analysis as a viable e-security measure.

This method is especially appealing for its relative ease of implementation, as the information needed to evaluate human typing patterns is already present in computers. The researchers do call for

additional testing before the new algorithm can be used as a security measure. "We concluded from the results presented that keystroke dynamics analysis holds big potential as an authentication method, but the methods used in the process have to be improved before it can be used as an independent security measure," they wrote.

**More information:** "A Secured and Reliable Biometric User Authentication Using Keystroke Template Method." *Journal of Applied Security Research* Volume 10, Issue 3, 2015 DOI: 10.1080/19361610.2015.1038767

Provided by Taylor & Francis