

Are Squiggly Lines the Future of Password Security?

Rutgers University



As more people use smart phones or tablets to pay bills, make purchases, store personal information and even control access to their houses, the need for robust password security has become more critical than ever. A new study shows that free-form gestures — sweeping fingers in shapes across the screen of a smart phone or tablet — can be used to unlock phones and grant access to apps. These gestures are less likely than traditional typed passwords or newer “connect-the-dots” grid exercises to be observed and reproduced by “shoulder surfers” who spy on users to gain unauthorized access.

“All it takes to steal a password is a quick eye,” said Janne Lindqvist, one of the leaders of the project and an assistant professor in Rutgers School of Engineering’s Department of Electrical and Computer Engineering. “With all the personal and transactional information we have on our phones today, improved mobile security is becoming increasingly critical.”

Lindqvist believes this is the first study to explore free-form gestures as passwords. The researchers will publish their findings in June as part of the proceedings of MobiSys '14, a premier international conference in mobile computing.

In developing a secure solution to this problem, Lindqvist and the other researchers from Rutgers and collaborators from Max-Planck Institute for Informatics, including Antti Oulasvirta, and University of Helsinki studied the practicality of using free-form gestures for access authentication. With the ability to create any shape in any size and location on the screen, the gestures had an inherent appeal as passwords. Since users create them without following a template, the researchers predicted these gestures would allow for greater complexity than grid-based gestures offer.

“You can create any shape, using any number of fingers, and in any size or location on the screen,” Lindqvist said. “We saw that this security protection option was clearly missing in the scientific literature and also in practice, so we decided to test its potential.”

To do so, the researchers applied a generate-test-retest paradigm where 63 participants were asked to create a gesture, recall it, and recall it again 10 days later. The gestures were captured on a recognizer system designed by the team. Using this data, the authors tested the memorability of free-form gestures and invented a novel method to measure the complexity and accuracy of each gesture using information theory. Their analysis demonstrated results favorable to user-generated, free-form gestures as passwords.

To put their analysis to practice, the Rutgers researchers then had seven computer science and engineering students, each with considerable experience with touchscreens, attempt to steal a free-form gesture password by shoulder surfing. None of the participants were able to replicate the gestures with enough accuracy, so while testing is in its preliminary stages, the gestures appear extremely powerful against attacks. While widespread adaptation of this technology is not yet clear, the research team plans to continue to analyze the security and management of free-form passwords in the future.

Source URL (retrieved on 05/27/2016 - 2:11pm):

<http://www.scientificcomputing.com/news/2014/06/are-squiggly-lines-future-password-security>