Scrambling against smudge attacks
11 June 2021, by David Bradley

So, how might one avoid a smudge attack? The obvious answer is to clean the phone's screen more frequently and immediately after entering a PIN, but a less "onerous" approach would be for the device itself to have a randomized keypad for unlocking. In a scrambled keypad, the numbers 0 to 9 would be arranged differently each time you go to unlock your phone, so there would be no build-up of your frequently smudged keys as it were and thus far less chance of a successful smudge attack.

At the moment, a scrambled keypad is not a feature of Android nor iOS devices. New work from a team in the U.S. published in the International Journal of Information and Computer Security, demonstrates how a scramble keypad might be implemented to protect smartphones from smudge attacks. Geetika Kovelamudi, Bryan Watson, Jun Zheng, and Srinivas Mukkamala of the New Mexico Institute of Mining and Technology, in Socorro, have carried out a usability and security study of a scramble keypad. They explain that it works perfectly to protect from smudge attacks. The scramble keypad also reduces the risk of someone illicitly gleaning your PIN by "shoulder surfing" (watching over your shoulder) while you tap it in, because the digits of the pad 0 to 9 will not be in the familiar places for their eye to quickly ascertain as you tap.

The implementation of a scramble pad would require very little additional coding to the touchscreen device's boot-up system but would offer a new level of protection from smudge attacks, a degree of protection from shoulder surfers, and potentially some protection from side-channel attacks.


Provided by Inderscience