

Scrambling against smudge attacks

11 June 2021, by David Bradley



Credit: CC0 Public Domain

The security-conscious among us use a PIN, a personal identification number, to "lock" our smartphones so that if the device is lost or stolen, a third party should not be able to access our contacts, messages, and other information held in myriad apps without a lot of effort to guess the PIN.

However, so many modern devices that hold our personal and business information are touchscreen and hackers and thieves are always resourceful. Picture the scene you give your phone screen a clean before tapping in your PIN to access your emails etc. The smudges left by your fingertips remain on the screen, marking out the likely numbers from the virtual keypad on your phone that you used to tap in your PIN.

Soon after, the phone is lost or stolen and that malicious third party carries out a "smudge attack"—they look at the screen and can have a good guess at the digits in your PIN and try them in various combinations pretty quickly. It is far easier to brute-force a four-digit PIN if you know the four digits rather than having to try all possible combinations of the numbers 0 to 9, after all!

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.

More information: Geetika Kovelamudi et al, On the adoption of scramble keypad for unlocking PIN-protected smartphones, *International Journal of Information and Computer Security* (2021). DOI: [10.1504/IJICS.2021.115345](https://doi.org/10.1504/IJICS.2021.115345)

Provided by Inderscience

APA citation: Scrambling against smudge attacks (2021, June 11) retrieved 28 October 2021 from <https://techxplore.com/news/2021-06-scrambling-smudge.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.