How Android unlocking patterns could be made more secure

July 23 2021

Credit: CC0 Public Domain

Users of Android devices can unlock the display by entering a pattern. This function is convenient and thus popular—however, less secure than locking with a PIN. An international research team thus recommends implementing a blocklist on Android devices that prohibits the 100 most

popular patterns, which are thus the easiest to guess. Precisely how this needs to be created has been investigated by Philipp Markert from the Horst Görtz Institute for IT Security at Ruhr-Universität Bochum together with colleagues from The George Washington University and the United States Navy.

The team led by Professor Adam Aviv from The George Washington University will be presenting the results at the USENIX Symposium on Usable Privacy and Security, which takes place from 8 to 10 August as a virtual conference. The data is available in advance as a freely accessible preprint.

What the most popular Android patterns look like

"While the four-digit PIN allows users 10,000 different combinations, there can theoretically be 389,112 versions of the Android patterns that are drawn on a three-by-three grid," explains Collins Munyendo, first author of the publication from The George Washington University. "However, users are not making the most of these options." In parts of the world where people read from the top left to the bottom right, patterns in the form of letters—such as a Z, L or W—are particularly popular. Around 49 percent of all patterns start in the top left; 32.5 percent end in the bottom right—this makes it easier for attackers to guess a pattern.

Various blocklists put to the test

In the current online study, the research team tested how blocklists of different lengths affect security and usability. They had 1,006 people select a new unlocking pattern. Some of the participants were able to select from all theoretically conceivable possibilities (control group); certain patterns were excluded for the other five groups, whereby five

blocklists of different lengths were used. If a user selected a blocklisted pattern, they were shown a warning and had to enter a new pattern.

The researchers had identified in an earlier study which were the most popular Android patterns. The shortest of the five tested blocklists contained the twelve most popular patterns from the previous study, the longest blocklist contained the 581 most popular patterns.

Blocklist with 100 patterns recommended

"The medium-length list with 100 blocklisted patterns is the best compromise between security and usability," summarizes Miles Grant from The George Washington University. With this blocklist, users took an average of 19 seconds to select a non-blocklisted pattern. As a comparison: a pattern was selected in 13 seconds in the control group. Once a pattern had been chosen, the users were able to remember it well: 99.54 percent correctly remembered the pattern they had set, while the figure was 100 percent in the control group.

Security increases, even with the shortest blocklist

The researchers also verified to what extent the blocklists affected the security of the patterns. They simulated how easily an attacker could guess the pattern of a stolen mobile phone. Without a blocklist, the chance of success was 23.7 percent after 30 attempted guesses. With the longest blocklist, it was 2.3 percent. The recommended list with 100 blocklisted patterns reduced the chances of success to around 7.5 percent.

"A blocklist with 100 entries would thus already significantly increase security, but require little extra effort from users during setup," summarizes Philipp Markert. "The layout with three-by-three grids,

which users know and like, would remain unchanged." In contrast to this, other ideas for improving the security of Android patterns included a four-by-four grid or a random arrangement of the grid dots on the display.

More information: Using a Blocklist to Improve the Security of User Selection of Android Patterns. www.usenix.org/conference/soup … resentation/munyendo

Provided by Ruhr-Universitaet-Bochum