Are we too predictable in our Android lock patterns?

August 23 2015, by Nancy Owano

After months—no, years— of security blogs telling us how dumb it is to choose easy to guess passwords such as password1234, we look for answers in ideas for strong authentication schemes. As for the Android pattern method of locking screens, one study coming from Norway suggests we're not exactly talking magic bullets.

Android lock patterns reveal a surprising degree of predictability. According to research, the patterns to lock and unlock Androids are not that complex. An overview of the research from Security Editor of *Ars Technica*, Dan Goodin, made the rounds of sites this week, when he reported "Data breaches over the years have repeatedly shown some of the most common passwords are "1234567", "password", and "letmein." Now, he said, a researcher's findings indicate that many Android Lock Patterns (ALPs) suffer a similar form of weakness.

Android Lock Patterns (ALPs) were welcomed in 2008 by many as a password alternative, taken as an innovative approach to lock your phone.

Sophos' John Zorabedian in *Naked Security* also noted that recently a researcher spent a year studying how people create lockscreen patterns, and she found interesting results.

Her study involved 3400 users and their selected lock patterns. Marte Løge, who is a technology analyst at Itera, presented her findings earlier this month at a conference in a talk titled "Tell me Who You Are and I Will Tell You Your Lock Pattern."

"A lockscreen pattern allows you to lock/unlock your device by swiping your finger on the screen - you draw a pattern that touches at least four and up to nine 'nodes.' With four-to-nine nodes, there are 389,112 possible patterns you could draw ," he wrote. That looks impressive but there is one problem, and it is entirely human.

Goodin of *Ars Technica* said that ALPs can contain as few as four nodes and a maximum of nine, but "Sadly, the minimum four-node pattern was the most widely created one by both male and female subjects, followed by five-node ALPs."

This human tendency shrinks the pool of available combinations. Goodin had more to report on her research results from the ALPs under analysis. "She found that a large percentage of them—44 percent—started in the top left-most node of the screen." Yet another factor making guessing easier is that more often than not, he added, patterns moved from left to right and top to bottom.

"More than 10 percent of the ones she collected were fashioned after an alphabetic letter, which often corresponded to the first initial of the subject or of a spouse, child, or other person close to the subject. The discovery is significant, because it means attackers may have a one-in-ten chance of guessing an ALP with no more than about 100 guesses."

Alex Drozhzhin in the Kaspersky Lab site noted another of her findings: People tend to use less strong patterns for their smartphones' lock screen then they use for online banking and even shopping apps.

Løge's suggestions to make ALPs more secure include choosing more nodes and higher complexity score and opening the Security category in Android settings and turning off the "make pattern visible" option.