Your Android device's Pattern Lock can be cracked within five attempts

January 23 2017

Credit: Lancaster University

The popular Pattern Lock system used to secure millions of Android phones can be cracked within just five attempts – and more complicated patterns are the easiest to crack, security experts reveal.

Pattern Lock is a security measure that protects devices, such as mobile phones or tablets, and which is preferred by many to PIN codes or text passwords. It is used by around 40 per cent of Android device owners.

In order to access a device's functions and content, users must first draw a pattern on an on-screen grid of dots. If this matches the pattern set by the owner then the device can be used. However, users only have five attempts to get the pattern right before the device becomes locked.

New research from Lancaster University, Northwest University in China, and the University of Bath, which benefitted from funding from the Engineering and Physical Sciences Research Council (EPSRC), shows for the first time that attackers can crack Pattern Lock reliably within five attempts by using video and computer vision algorithm software.

By covertly videoing the owner drawing their Pattern Lock shape to unlock their device, while enjoying a coffee in a busy café for example, the attacker, who is pretending to play with their phone, can then use software to quickly track the owner's fingertip movements relative to the position of the device. Within seconds the algorithm produces a small number of candidate patterns to access the Android phone or tablet.

The attack works even without the video footage being able to see any of the on-screen content, and regardless of the size of the screen. Results are accurate on video recorded on a mobile phone from up to two and a half metres away – and so attacks are more covert than shoulder-surfing. It also works reliably with footage recorded on a digital SLR camera at distances up to nine metres away.

Researchers evaluated the attack using 120 unique patterns collected from independent users. They were able to crack more than 95 per cent of patterns within five attempts.

Complex patterns, which use more lines between dots, are used by many to make it harder for observers to replicate. However, researchers found that these complex shapes were easier to crack because they help the fingertip algorithm to narrow down the possible options.

During tests, researchers were able to crack all but one of the patterns categorised as complex within the first attempt. They were able to successfully crack 87.5 per cent of median complex patterns and 60 per cent of simple patterns with the first attempt.

Researchers believe this form of attack would enable thieves to access phones after pinching them to obtain sensitive information, or would allow malware to be quickly installed on devices while their owners were distracted.

In addition, given people often use the same pattern across multiple devices a pattern obtained from one device could be used to access a second device.

Dr Zheng Wang, principle investigator and co-author of the paper, and Lecturer at Lancaster University, said: "Pattern Lock is a very popular protection method for Android Devices. As well as for locking their devices, people tend to use complex patterns for important financial transactions such as online banking and shopping because they believe it is a secure system. However, our findings suggest that using Pattern Lock to protect sensitive information could actually be very risky."

"Contrary to many people's perception that more complex patterns give better protection, this attack actually makes more complex patterns easier to crack and so they may be more secure using shorter, simpler patterns," Guixin Ye, the leading student author from Northwest University, added.

The researchers have proposed suggested countermeasures to prevent this attack. They include device users fully covering fingers when drawing the pattern; or pattern lock designers mixing pattern locking with other activities such as entering a sentence using Swype-like methods; in addition having the screen colour and brightness change dynamically could confuse the recording camera.

More information: Ye, Guixin and Tang, Zhanyong and Fang, Dingyi and Chen, Xiaojiang and Kim, Kwang In and Taylor, Ben and Wang, Zheng (2016) Cracking Android pattern lock in five attempts. In: The Network and Distributed System Security Symposium 2017 (NDSS'17). http://www.research.lancs.ac.uk/portal/en/publications/-(9d47cd22-a76a-4cf0-b35c-aaf8f1a2f102).html

Provided by Lancaster University