Hackers could guess your smartphone PIN with sensor data: NTU researchers

SINGAPORE: The data collected from the sensors on your smartphone could be used to hack into your device, researchers at the Nanyang Technological University announced on Tuesday (Dec 26). This, they said, highlights a "significant flaw" in smartphone security.

According to their research published in Cryptology ePrint Archive, hackers can guess the security PIN of a smartphone and unlock it just by using data from the device's physical sensors such as accelerometer, gyroscope and ambient light sensor, an NTU news release said.

The sensors are openly available for all apps to access, and require no permissions to be given by the phone user, representing a potential security vulnerability, it added.

"Using a combination of information gathered from six different sensors found in smartphones and state-of-the-art machine learning and deep learning algorithms, the researchers succeeded in unlocking Android smartphones with a 99.5 per cent accuracy within only three tries, when tackling a phone that had one of the 50 most common PIN numbers," the release said.

The previous best phone-cracking success rate was 74 per cent for the 50 most common pin numbers, but NTU's technique can be used to guess all 10,000 possible combinations of four-digit PINs, it added.

The researchers also told Channel NewsAsia in a follow-up email that their method can be applied to PINs that go beyond four digits.

CRACKING THE CODE

The researchers, led by NTU senior research scientist Dr Shivam Bhasin, used sensors in a smartphone to model which number had been pressed by its users, based on how the phone was tilted and how much light is blocked by the thumb or fingers. The sensors were the accelerometer, gyroscope, magnetometer, proximity sensor, barometer, and ambient light sensor.

With data collected from three people, who entered a total of 210 random four-digit pin numbers on the phone, the custom application developed by the researchers recorded the relevant sensor reactions. The app, with its deep learning algorithm, was then able to give different weightings of importance to each of the sensors, depending on how sensitive each was to different numbers being pressed.
That helped to eliminate factors which it judges to be less important and increased the success rate for PIN retrieval.

"So while a malicious application may not be able to correctly guess a PIN immediately after installation, using machine learning, it could collect data from thousands of users over time from each of their phones to learn their PIN entry pattern and then launch an attack later when the success rate is much higher," the researchers said.

They added that the method has only been tested on the Android platform, but "to to the best of their knowledge", the sensor data is available to any app that wants to access it on both Android and iOS.

Professor Gan Chee Lip, director of the Temasek Laboratories at NTU, said: "Along with the potential for leaking passwords, we are concerned that access to phone sensor information could reveal far too much about a user’s behaviour. This has significant privacy implications that both individuals and enterprises should pay urgent attention to."

The researchers did not reply directly when asked if Google was notified of the finding. They did note that the research was published online in an open archive since Dec 6 and they have submitted the paper to a cybersecurity conference that will be held next year.

To keep mobile devices secure, Dr Bhasin advised users to have passcodes of more than four digits, coupled with other authentication methods like one-time passwords, two-factor authentications, and fingerprint or facial recognition.

The researchers also said their findings suggest that sensor data should be protected, like how GPS data is currently, in order to further safeguard user privacy.