Warning: Hackers can guess your phone PIN by accessing its sensor data

By James Lu - on 26 Dec 2017, 2:34pm

According to researchers from Nanyang Technological University, your smartphone's accelerometer, gyroscope and proximity sensors could be used by hackers to guess your security PIN.

Led by Dr Shivam Bhasin, NTU Senior Research Scientist at the Temasek Laboratories at NTU, the team found that information gathered from six different sensors on the phone combined with state-of-the-art machine learning and deep learning algorithms could be used to unlock Android smartphones with a 99.5 percent accuracy within only three tries when tackling a phone that had one of the 50 most common PIN numbers.

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

The researchers used the sensor data in the phone to determine 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.

“When you hold your phone and key in the PIN, the way the phone moves when you press 1, 5, or 9, is very different. Likewise, pressing 1 with your right thumb will block more light than if you pressed 9,” explains Dr Bhasin, who spent ten months with his colleagues, Mr David Berend and Dr Bernhard Jungk, on the project.

The researchers, who have had their findings published in Cryptology ePrint Archive on 6th December, believe their work highlights a significant flaw in smartphone security, as using the sensors within your phone generally requires no permissions to be given by the user and are openly available for all apps to access.

Dr. Bhasin recommends that users keep themselves safe by using PINs with more than four digits, coupled with other authentication methods like one-time passwords, two-factor authentications, and fingerprint or facial recognition.