Name: Ziheng Xu

UID: 704756821

TA: Aditi Mithal

10 March 2018

NTU study finds that hackers could guess your phone PIN using its sensor data

As smartphones with various kinds of Apps are making our lives more and more convenient and productive, modern people today might claim that they cannot even live without their phones. However, at the same time, privacy and security on those portable devices have also raised considerably large amounts of concerns among the public. Recently, researchers at Nanyang Technological University, Singapore (NTU) finds that hackers can guess people's phone PIN combination using the data collected by six sensors on our smartphones.

The potential vulnerability exists because of relatively easy access to the data collected from six sensors on our smartphones, accelerometer, gyroscope, magnetometer, proximity sensor, barometer, and ambient light sensor. Accelerometer detects the orientation of devices by measuring the linear acceleration. Gyroscope functions similarly, but measures the angular velocity to detect three dimensional movement. Magnetometer measures Earth magnetism and assists GPS in navigations. Barometer improves two dimensional map by adding the altitude there. Proximity sensor detects

nearby objects without physical contact. And ambient light sensor measures the amount of light in the environment and adjusts the brightness of the screen accordingly. When users typed in their PIN passwords, a combination of information is gathered from those six sensors, like how they tilted the phone or the amount of light being blocked according to how the users are typing in their password. For example, the thumb is very likely to block more light if the user is pressing the key '1' instead of the key '9'. This can give us clues to possible users' passwords. Data from six sensors would be put on weights based on how users tend to use the phone. Those information would be processed further and under machine learning to generate a pattern and eventually guess the correct password. According to the paper, the accuracy rate in unlocking a Android phone using one of the 50 the most common 4 digit password is 99.5 percent in three tries. Different people might type in their passwords differently, but there are still tendencies to follow. For example, people are more likely to type in their PIN using the thumb, and probably the one of their right hand since that's the only way if you want to unlock your phone using one hand.

The significance of this vulnerability will become larger as companies, are developing increasing number of new sensors on their products to add additional features, like the new FaceID sensor inside the notch of iPhone X from Apple for example. Surprisingly, those sensors are easily accessed by App developers and there are few ways for users to give permissions regarding using their sensors and actually this range of sensors are called zero-permission sensors. According to the record on statista.com, there are approximately 222.9 million iPhone users in US alone. The algorithm might not be able to figure out the PIN combination in one hit, but if it keeps running in background, it is able to collect a lot of data and eventually crack open our personal cell phones. And large population of users gives enough data for this algorithm to find a pat-

tern that people tend to use in typing PIN combination. Not to mention, a lot of users choose to have their devices jail broken so that they can try some extra cool features by using untrusted applications developed by third parties, which puts the security of their devices into even deeper danger. Those malicious third party Apps are not censored since Apple might not have the power to ban them if they are not under App store.

My opinion towards this paper is this vulnerability should really raise the public awareness against smartphone security and privacy. Usually, we do not consider ourselves as possible targets of hacking acts since we are just ordinary people who might not be that rich or hold significant positions in the society. However, in the case here, the exploit collects data from general public users to generate such a good pattern so that it can be used to unlock other people's personal phones with a accuracy rate of 99.5%. The hackers might not directly attack our devices, but our data gradually contribute to their algorithms, so when they want, they would be able to attack someone's device easily with our help. Anyone could potentially be the target without even noticing the existence of this exploit in his or her phone. The implication of those zero-permission sensors goes way beyond just guessing the PIN number, since it can also give a lot of private information regarding users's location, behavior and so on…

There are a few ways we can avoid being attacked by this exploit. First, we can use more complicated password pattern instead of the simple 4 digit one. We might also use the gesture unlock, voice unlock, or Touch ID instead of directly typing in the password. Moreover, just like what UCLA login has asked us to do, we might use mechanisms like '2 Factor Authentication' so that even if the password is compromised, the account should still be safe. Second, I believe Android and iOS should give some restrictions to the extent sensors are being used to app developers' perspective, or at least the users could have the right to give permission to using their sensors only on apps they

trusted. Since the danger lies deeper for the sensor problem, beyond just the password leakages, hackers might be able to pull out private information like location or behaviors, which would be somehow even worse.

Work Cited

Berend, David, et al. “There Goes Your PIN: Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting.” Open Access, 5 Dec. 2017, pp. 1–19, eprint-.iacr.org/2017/1169.

NTU Study Finds That Hackers Could Guess Your Phone PIN Using Its Sensor Data. Edited by Lester Kok, 26 Dec. 2017, media.ntu.edu.sg/NewsReleases/Pages/newsdetail.aspx?news=e57faffc-24ea-4034-9181-f5fea9850690.