Poster Abstract: Side Channel Attack on Smartphone Sensors to Infer Gender of the User

Shirish Singh
shirish@cs.columbia.edu
Columbia University
New York City, NY

Devu Manikantan Shila
devums@unknot.id
Unknot.id
Orlando, FL

Gail Kaiser
kaiser@cs.columbia.edu
Columbia University
New York City, NY

ABSTRACT

Smartphones incorporate a plethora of diverse and powerful sensors that enhance user experience. Two such sensors are accelerometer and gyroscope, which measure acceleration in all three spatial dimensions and rotation along the three axes of the smartphone, respectively. These sensors are used primarily for screen rotations and advanced gaming applications. However, they can also be employed to gather information about the user's activity and phone positions. In this work, we investigate using accelerometer and gyroscope as a side-channel to learn highly sensitive information, such as the user's gender. We present an unobtrusive technique to determine the gender of a user by mining data from the smartphone sensors, which do not require explicit permissions from the user. A preliminary study conducted on 18 participants shows that we can detect the user's gender with an accuracy of 80%.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**.

KEYWORDS

Privacy, Smartphone, Sensors, Gender detection

1 INTRODUCTION

Most mobile devices, including smartphones, tablets, and smartwatches, come equipped with built-in sensors such as accelerometer, gyroscope, and magnetometer. A study suggests that accelerometers are the most widely used sensor accessed by mobile apps [1]. Accelerometer and gyroscope sensors measure acceleration and rotation forces caused by the movements and vibrations of an object. When the smartphone goes from a standstill to any velocity, the accelerometer is designed to respond to the vibrations associated with such movements. Similarly, when the smartphone rotates about any of the smartphone axes, the gyroscope captures that change. The axes of acceleration and rotation are shown in Figure 1.

The privacy implications of inferences from smartphone sensors have previously been reviewed in [5]. For example, [6] showed how to infer the user's gender from their hip movements, gait, and physical activity patterns while walking for five to ten minutes with the phone in their pocket. Instead, we observe that male and female participants hold their phones differently. We collect accelerometer and gyroscope sensor data from the user's smartphone while the user is reading or browsing the internet, which enables detecting the user's gender within 30 seconds with high confidence. This difference in the holding pattern between the user groups stems from user's hand stability. Gender differences in hand stability were earlier reported in a medical journal [3].

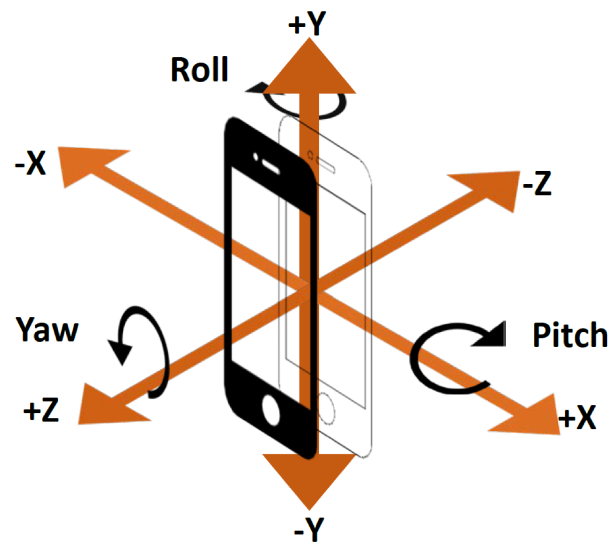

Figure 1: The x, y, and z-axis represent the horizontal axis along the face of the phone, the vertical axis along the face, and the axis along the perpendicular plane passing through the center of the phone, respectively. Figure from [4].

Since these holding patterns are subliminal in nature, it is difficult to replicate these patterns consciously. The difference becomes evident in the plots of sensor readings corresponding to both genders. Figures 2 and 3 show the differences in the accelerometer and gyroscope readings of randomly selected male and female participants from our study. These variations in the sensor readings contribute to differences in the phone holding pattern in the genders.

2 METHODOLOGY

We developed an Android application to collect the smartphone sensor data that captures the subtle hand movements of the participant. In our study, we use accelerometer and gyroscope sensors, which allow us to infer the hand movement and rotation along the three axes of the smartphone sensors.

We designed the app to collect data from the sensors at a frequency of 50 Hertz (one sample after every 20 milliseconds). In

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

SenSys '19, November 10–13, 2019, New York, NY, USA

© 2019 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-6950-3/19/11…$15.00
https://doi.org/10.1145/3356250.3361939

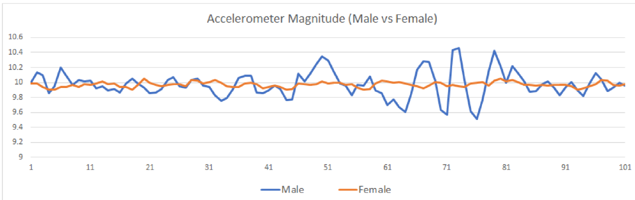

Figure 2: Accelerometer magnitude graph of male and female participants show the subtle differences in the phone holding characteristics of the two genders. The graph shows that the female participant's hand is more stable as compared to that of the male.

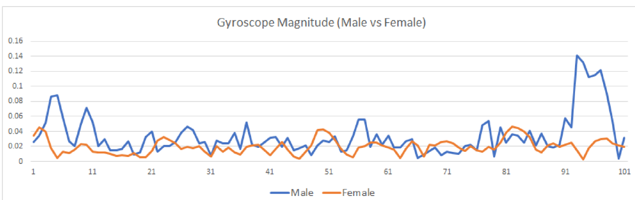

Figure 3: Gyroscope magnitude graph of male and female participants show the variation in the phone holding pattern. The data from the male have higher average magnitude with more fluctuations as compared to the female.

our study, a combination of accelerometer and gyroscope sensors demonstrated good results on the gender detection task. We recruited nine male and nine female participants (so far) in our study. Every participant was asked to read a short passage on an Android device (Samsung Galaxy S9) while holding the phone in either one hand or both hands, according to their preference. We allowed the participants to be comfortable in standing/sitting posture without using any arm support.

We gather raw X, Y, and Z-axis readings from each sensor. In addition to the raw data, we computed the magnitude of accelerometer and gyroscope from the raw sensor data. Then, for each raw and processed data value, we applied the Tsfresh library [2] to extract time-series features. Our dataset consists of 160 features comprising of 20 Tsfresh metrics calculated for eight raw and processed sensor data. We applied Principal Component Analysis (PCA) dimensionality reduction on the data before training the models.

3 RESULTS

We obtained the best results with a window size of 100 samples (2 seconds of sensor data collected at 50 Hz). Essentially, we represent two seconds of data using a feature vector comprising of the Tsfresh features computed using the raw and processed sensor measurements. On average, every user contributed about 2000 Tsfresh samples, which is equivalent to 40 seconds of data.

We evaluated our work through the following strategy: Given n users, we use the data from the $n-1$ participants for training the gender detection model and tested using n^{th} participant. We applied four algorithms for the classification task.

Using the one user vs. others for testing, we achieved 83% accuracy for 18 participants. Overall, we achieved 89% detection accuracy for female participants and 78% accuracy for male participants. The ROC curve of 10-fold cross-validation is shown in Figure 4.

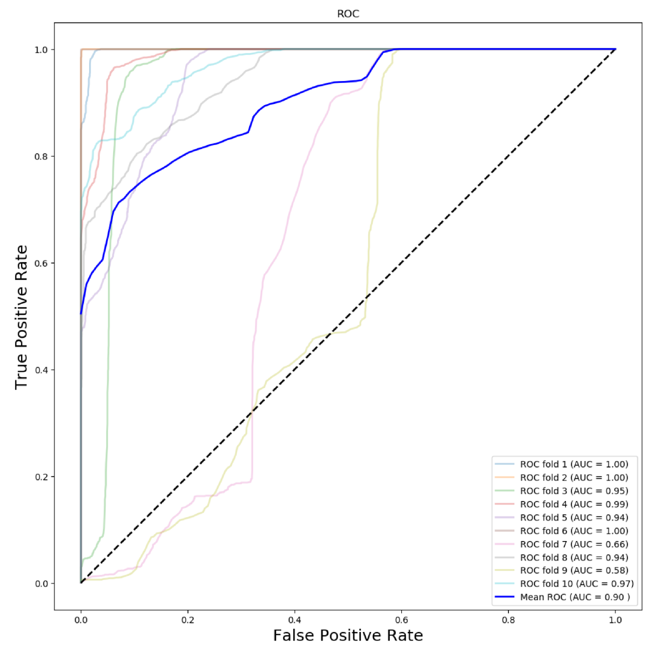

Figure 4: ROC curve of 10-fold cross validation

4 CONCLUSION

Sensors like accelerometer and gyroscope do not require explicit permission on the smartphone but have the potential to gather information about the user. This study presents a non-invasive transparent technique to infer the gender of the user by mining data of the smartphone sensors.

ACKNOWLEDGMENTS

The Programming Systems Laboratory is supported in part by NSF CNS-1563555, CCF-1815494 and CNS-1842456.

REFERENCES

[1] Xiaolong Bai, Jie Yin, and Yu-Ping Wang. 2017. Sensor Guardian: prevent privacy inference on Android sensors. *EURASIP Journal on Information Security* 2017, 1 (2017), 10.

[2] Maximilian Christ, Nils Braun, Julius Neuffer, and Andreas W. Kempa-Liehr. 2018. Time Series FeatuRe Extraction on basis of Scalable Hypothesis tests (tsfresh âĂŞ A Python package). *Neurocomputing* 307 (2018), 72 – 77.

[3] Hiroshi Endo and Koichi Kawahara. 2011. Gender differences in hand stability of normal young people assessed at low force levels. *Ergonomics* 54, 3 (2011), 273–281.

[4] Chris Hemedinger. 2018. Using your smartphone accelerometer to build a safe driving profile. https://blogs.sas.com/content/sgf/2018/09/26/accelerometer-driving-profile/

[5] Jacob Leon Kröger, Philip Raschke, and Towhidur Rahman Bhuiyan. 2019. Privacy Implications of Accelerometer Data: A Review of Possible Inferences. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP '19)*. ACM, New York, NY, USA, 81–87.

[6] Gary M Weiss and Jeffrey W Lockhart. 2011. Identifying user traits by mining smart phone accelerometer data. In *Proceedings of the fifth international workshop on knowledge discovery from sensor data*. ACM, 61–69.