# ACM HotMobile 2013 Poster: Leveraging Imperfections of Sensors for Fingerprinting Smartphones

**Sanorita Dey** *deys@email.sc.edu*
**Nirupam Roy** *royn@email.sc.edu*
**Wenyuan Xu** *wyxu@cse.sc.edu*
**Srihari Nelakuditi** *srihari@cse.sc.edu*
CSE Department, University of South Carolina, Columbia, SC, USA

*Device fingerprinting, similar to that of humans, if done well, can provide a convenient form of identification. In this poster, we explore whether constituent hardware sensors like accelerometers and gyroscopes of different smartphones can be exploited to fingerprint a smartphone. We observe that the readings of these sensors exhibit diverse features for different smartphones consistently when subjected to the same action.*

## I. Introduction

Many applications tend to allow automated login by storing passwords/cookies on the smartphone. While convenient for users, this approach is vulnerable to duplication and distribution of the password/cookie to another device. As an alternative to passwords/cookies, recently there have been efforts to fingerprint devices for identification and authentication [3]. Towards that end, we explore whether it is possible to fingerprint a smartphone using its built-in hardware sensors such as accelerometers. As a case study, we consider accelerometer as it is commonly found in smartphones. Smartphone accelerometers are based on Micro Electro Mechanical Systems. This electro-mechanical structure can introduce subtle idiosyncrasies in different accelerometer chips. For an example, a small gap between structural parts due to the manufacturing process can change the capacitance [1] of the accelerometer chip which is used to measure the acceleration. Moreover accelerometer chips use Quad Flat Non-leaded or Land Grid Array packaging, another source of imperfections [2]. We propose `SensorPrint` to leverage such imperfections of sensors.

## II. Do Sensors Have Fingerprints?

The underlying premise behind `SensorPrint` proposal is that sensors exhibit diverse behavior. The aforementioned subtle imperfections in accelerometer chips of the same model can lead to different acceleration values, yet not affect the rated performance of the target applications. To justify this intuition, we conducted an initial experiment where fifteen smartphones were stimulated in an identical pattern with their own internal vibration motors and their accelerometer readings are recorded.

Figure 1 shows the mean RSS versus the standard deviation for six devices among the fifteen devices. Each repetition of the experiment on a smartphone yields a point and the points from multiple experiments on the same device form a cluster in this graph. It appears that most of the devices in Figure 1 can easily be distinguished as they form distinct clusters, but not the two nexus S devices (on the top-left side) as they form somewhat overlapping clusters.

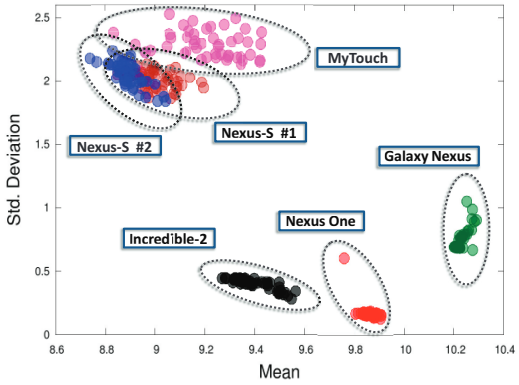


Figure 1: Accelerometer responses of six different devices for the same stimulation. Only the two Nexus S devices' accelerometer values appear indistinguishable.

We find that even those devices can be separated when we consider another feature called the spectral flatness, which measures the distribution of power in all the spectral bands. If power is equally distributed in all the spectral bands, then spectral flatness becomes high. On the other hand, if the power is concentrated in a small subset of spectral bands, then spectral flatness becomes low. Figure 2 shows the spectral flatness of the accelerometer readings of the two Nexus S devices, where one device consistently shows a larger spectral flatness than the other, even though their hardware settings as well as the the operating system are

the same.

This shows that two devices that appear indistinguishable according to some features could be separated using some other appropriate features. However applying more features can improve the accuracy of the verification process. In our system we use 40 different features to distinguish smartphones from each other. This implies that imperfections of smartphone sensors yield diverse features, which when harnessed carefully, can help fingerprint it. Based on this observation, we propose the basic design of the `SensorPrint` system.

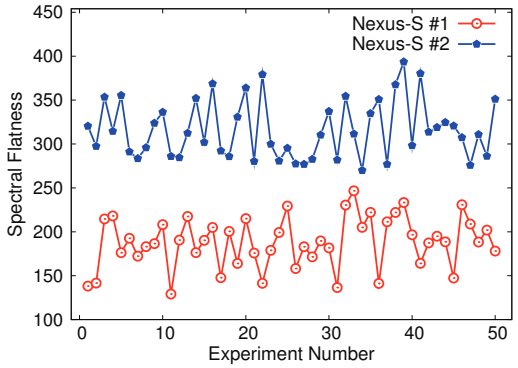


Figure 2: Two Nexus S devices that are indistinguishable in Figure 1 exhibit distinct spectral flatness.

## III. Design Overview

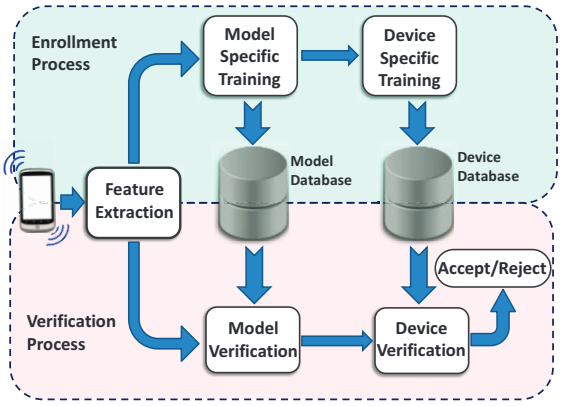


Figure 3: `SensorPrint` design overview. `SensorPrint` consists of two phases: enrollment and verification. `SensorPrint` employs two-round verification: verify the model of the smartphone first and then the smartphone.

The very first step in building the `SensorPrint` system is to obtain a smartphone's fingerprint. The system should then be able to check the veracity of any device by matching the sensor readings from that device against the claimed phone's fingerprint. Figure 3 depicts this process consisting of an enrollment phase and a verification phase. During an enrollment, `SensorPrint` applies a specific stimulation, collects sensor readings from the phone, extracts key features those constitute its fingerprint, and registers the phone with its fingerprint. For verification, `SensorPrint` applies the same stimulation to the device being verified, collects sensor readings, extracts the same set of features, and verifies whether these features match the stored fingerprint. It performs verification in two steps: first it verifies the model of a smartphone using a light-weight method and then the individual identity of the phone is verified with the rich set of features.

## IV. Ongoing Work

We are currently using Pearson Correlation Coefficient to measure the similarity of sampling interval of the accelerometer readings to separate the devices of different models. In future we need to explore how energy efficiency the system is in terms of power. We also need to investigate the effect of CPU load and operating system on the fngerprint of the smartphones. Besides this, we are also studying the scalability of this scheme. Our preliminary evaluation of `SensorPrint` shows that it can verify a smartphone with an accuracy of more than 96%.

These initial results encourage us to conduct further investigation and also explore other sensors such as gyroscope for fingerprinting mobile devices.

## V. Conclusion

`SensorPrint` is just an initial effort which shows the feasibility of smartphone identification by harnessing various ulterior features of accelerometer data obviating the requirement of external setup. More works need to be done to explore whether other sensors available at smartphones can also be used for fingerprinting devices.

## References

[1] ANDREJAIC, M. Mems accelerometers. *Seminar* (March 2008).

[2] HILLMAN, D. C., AND TULKOFF, C. Manufacturing and Reliability Challenges With QFN. *SMTA DC Chapter 45*, 1 (February 2009).

[3] JASON FRANKLIN ET AL. Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. In *USENIX Security* (August 2006).