Leveraging Imperfections of Sensors for Fingerprinting Smartphones

Sanorita Dey, Nirupam Roy, Wenyuan Xu, Srihari Nelakuditi
Computer Science & Engineering, University of South Carolina

1 Introduction

Many applications tend to allow automated login by storing passwords/cookies on the smartphone. As an alternative, recently there have been efforts to fingerprint devices for identification and authentication [2]. Towards that end, we explore whether it is possible to fingerprint a smartphone using its built-in hardware sensors such as accelerometers. Smartphone accelerometers are based on Micro Electro Mechanical Systems whose structure introduces subtle idiosyncrasies due to the manufacturing process. Moreover accelerometer chips use Quad Flat Non-leaded or Land Grid Array packaging, another source of imperfections [1]. We propose `SensorPrint` to leverage such imperfections of sensors.

2 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 randomly chosen 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.

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 brands. 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.

3 Ongoing Work

We are currently considering 40 features of accelerometer data both in the time and frequency domain to capture the diversity among smartphones. We are also using Pearson Correlation Coefficient to measure the similarity of sampling interval of the accelerometer readings to separate the devices of different models. 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.

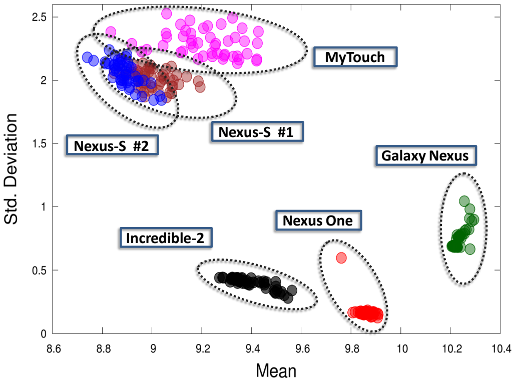

Figure 1: Accelerometer responses of six different devices for the same stimulation. Only the two Nexus S devices' accelerometer values appear indistinguishable.

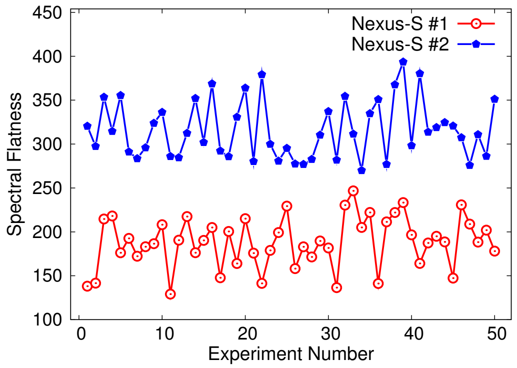

Figure 2: Two Nexus S devices that are indistinguishable in Figure 1 exhibit distinct spectral flatness.

4 References

[1] Hillman, D. C., and Tulkoff, C. Manufacturing and Reliability Challenges With QFN. *SMTA DC Chapter 45*, 1 (February 2009).

[2] Jason Franklin et al. Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. In *USENIX Security* (August 2006).