POSTER: Mobile Device Identification by Leveraging Built-in Capacitive Signature

Manh Huynh[1], Phuc Nguyen[1], Marco Gruteser[2], Tam Vu[1]
[1]MNS Lab, University of Colorado Denver ,[2] WINLAB, Rutgers University
[1]{huynh.manh, phuc.v.nguyen, tam.vu}@ucdenver.edu
[2]gruteser@winlab.rutgers.edu

ABSTRACT

This work presents *on-top*, a new device identification method that exploits off-the-shelf capacitive touchscreen to extract its capacitive signature. The method relies on a key observation that each capacitive touch screen has a *unique* capacitive signature, which is caused by either the difference in touch sensing technologies or the imperfections of the sensor during its fabrication. In particular, the voltage pattern generated by commercial off-the-shelf (COTS) capacitive touchscreens during finger touch sensing is uniquely identifiable. Our preliminary evaluation with actual hardware prototype on 14 mobile touchscreens shows that *on-top* achieves a promising performance of 100% detection rate without any false positive. We also show that *on-top* can be used to securely trigger wireless communication while it consumes a very little amount of power (38.18 times lower than triggering using Near Field Communication (NFC) and 18.28 times lower than using Bluetooth low energy (BLE)).

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Authentication

Keywords

Device Identification; Capacitive Signal; Signature

1. INTRODUCTION

Capacitive touchscreens are becoming more and more pervasive. One could easily find them in smart mobile devices such as smart phones, tablets, smart watches among others, in ATM machines, or even in the touch pad of an old laptop, just to name a few. Motivated by the pervasiveness of this technology, we explore a new method, *on-top*, to extract and recognize hardware fingerprints of COTS devices that are equipped with capacitive touchscreen. These hardware fingerprints are useful for various applications, a few of which are discussed in the latter part of this section.

On-top is based on the touch sensing principle of today's capacitive touchscreens. While the original role of capacitive sensing is to scan and detect for human finger touch events, we have leveraged these signals for hardware signature extraction and recognition. In particular, the voltage pattern generated by a touchscreen to sense human touch exhibits a unique set of feature between devices, even when those devices are from the exactly the same manufacturer and of the same batch. This uniqueness is due to the diversity of touch controller and touch sensor technologies in combination with the inevitable manufacturing imperfections of the touchscreen and touch sensors.

CCS'15, October 12–16, 2015, Denver, Colorado, USA.
ACM 978-1-4503-3832-5/15/10.
DOI: http://dx.doi.org/10.1145/2810103.2810118 .

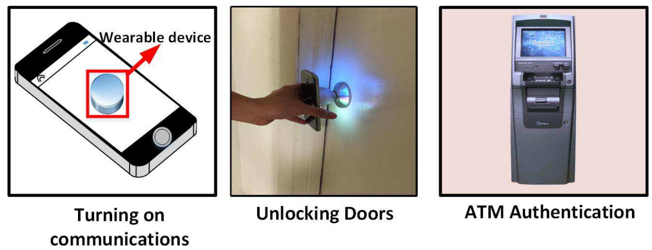

Figure 1: The example application utilizing capacitive screen signatures.

With *on-top*, a device can be identified when its capacitive signature is extracted. The left-most picture on Figure 1 shows an example of using *on-top* for authentication. In this case, a wearable device (such as a heart-rate tracker and health monitor) wants to be able to verify the identity of the mobile device before starting communicating sensitive information (health information, for example) to the mobile device. It would first be placed on top of the touchscreen of the mobile device. The wearable device has a conductive case that could capture voltage coming out of the touch screen. We note that this voltage is always generated by the screen to sense human touch regardless of the present of a human finger on the screen. Upon receiving such voltage time series, the wearable device extracts spectral and tempo features of the time series to construct a unique signature of the device. This signature is then used to identify the screen and, therefore, identify the mobile device that has screen on.

In this example, no wireless communication is needed until the wearable recognizes the mobile device. In addition, the mobile device does not need to explicitly transmit its identification to the wearable, which results in (1) a higher level of security against eavesdropping and man-in-the-middle attacks and (2) saving energy for identification. It is important to note that the energy saving is significant since, otherwise, the host must also wirelessly transmit beaconning signals even without the presence of the wearable. The second application (the second sub-figure of Figure 1) is leveraging the capacitive screen signature of mobile phone as a electronic key. Currently, some of the transferring electronic keys are employed in smart home instead of using the metal keys. The electronic token is sent from a mobile device using wireless sig-

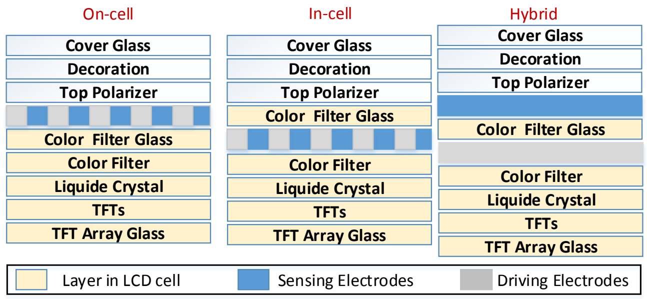

Figure 2: Different sensor locations found in today's smart phone/tablets.

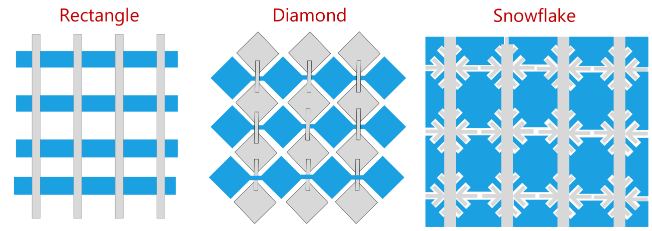

Figure 3: Example of different conductor patterns.

nals such as WiFi, Bluetooth, or NFC to smart lockers. These techniques are not completely secure because of their wireless connectivity-based features, which are prone to eavesdropping and relaying attack. The main advantage of *on-top* on this application scenario is that it does not require any wireless communication channels to transfer electronic keys so that it promises to be more secure. The third application is ATM transaction authentication. The capacitive screen of the ATM captures the signature of user's device which can be used to replace the traditional PIN number. Furthermore, the ATM machine with capacitive touch screen in turn could also be recognized by the user's device before the device start transmitting important information.

Our contributions are three folds: (1) We are the first to realize and make use of the built-in capacitive signature of COTS devices.(2) We prototyped and implemented the preliminary system which includes a hardware prototype, voltage signal collection and segmentation, feature extraction and selection, and machine learning algorithms to show the feasibility of the system. (3) We present the preliminary results and identify the next plausible steps in realizing this hardware fingerprinting method which sets a foundation for many communication triggering and identification applications on capacitice touch-enabled devices to come.

2. SOURCES OF CAPACITIVE SCREEN SIGNATURE

This section takes a close look at different sensing technologies, possible manufacturing imperfections, and different touch controllers and touch sensors embedded on today's smartphones to explain the sources of capacitive screen signatures. These diversities and subtle differences alter the voltage patterns being sent out from the screen for sensing touches. These very altered patterns are however stable within each devices, making them suitable as a form of hardware fingerprinting. On one hand, the *physical construction* of touch screens differs in one or more of the following 5 aspects: sensor layering structures, sensor locations, sensor patterns, electrode materials and manufacturing imperfections. On the other hand, the *logical construction* of touch screens mainly differs in the way that the sensing signal is controlled such as sampling frequency, clock skew, and charging time. The combination of these difference makes up a unique signature for each screen.

Sensor layering structures, which describe different layers of a sensor, are classified into three types: glass-only structures, glass-and-film structures, and film-only structures. Among of these structures, film-only touch sensor is most commonly used [4] since it makes the mobile devices thinner, lighter and also easier to be layered.

Sensor locations, which represent the position of the sensor relative to display cells (e.g. LCD crystal cell), are also categorized into three types: on-cell, in-cell, and hybrid structures, as shown in Fig. 2. For example, in on-cell technology, the touch sensors are deposited on the top of color filter glass or the encapsulation glass and under the polarizer. In contrast, in-cell sensors, which are deposited inside LCD cell, produce the thinnest devices and also deliver the lowest cost solution today.

Sensor patterns, which describe the arrangement of electrodes on screen, include triangles, diamonds, snowflakes, streets and alleys, telephone poles [5]. Fig. 3 shows three examples of sensor patterns, in which the blue electrodes are driving sensors (i.e. sending out signal) and the grey electrodes are sensing ones. Diamond pattern for example is commonly found in Apple smart devices [1].

Electrode materials could be ITO (Indium Tin Oxide), metal, silver nanowire, carbon nanotube, conductive polymer, and graphene. A good electrode material should have low resistance so that it has small charging time and discharging time, which in turn make the sensor more responsive.

Manufacturing imperfections of these tiny touchscreen sensors are arisen from the slight wears of the manufacturing machines, changes in temperature and humidity at the time of manufacturing, or minor variations of the sensor's chemical compositions. This could cause a distortion and nonuniformity of physical properties of sensors even within the same batch.

Logical construction of touch screens is regulated by its touch sensing controllers, each of which might run different algorithms or have a different set of execution parameters. Each manufacturer has it own family of (sometime proprietary) touch sensing algorithms. Examples include CapSense Sigma Delta modulation of Cypress, Relaxation Oscillator of Silicon labs, or Capacitive Voltage Divider of Microchip. This diversity is one of many sources of capacitive signature. Moreover, even when the exactly same algorithm is applied, clock skew or synchronization imperfection of touch controller could differ one controller from the others. This phenomenon arises because of many different factors such as wire-interconnect length, temperature variations, material imperfections in manufacturing process.

3. SYSTEM DESIGN

3.1 Design Goals and Challenges

On-top is designed to meet the the following goals: high detection rate, robust to its dynamic operating environment. To achieve these goals, there are three main challenges need to be considered:

Weak Signal Strength: Since the ground of mobile devices and wearable devices is coupled through earth ground, it weakens the signal strength. We try to amplify the signal strength by designing an amplifier circuit.

Highly noisy and dynamic operating environment: Noise removal using bandpass filter is first applied to increase the robustness in the signature segmentation. The feature selection algorithm

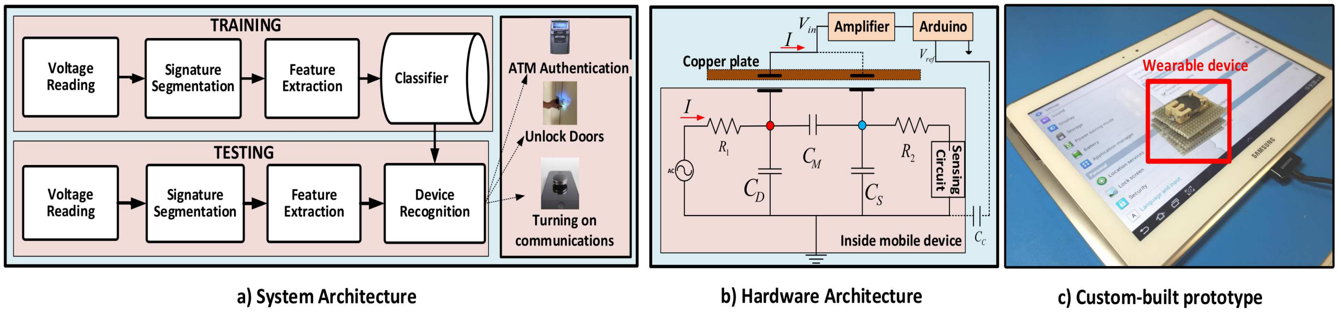

Figure 4: The system architecture, hardware architecture and custom-built prototype of *on-top*.

are carefully designed and executed to explore the best features that overcome the instability voltage signal captured from the screen.

Negative voltage signal reading consumes much energy: We design a bipolar to unipolar converter to capture voltage signal on both signs without consuming a large amount of energy.

3.2 System design

This section describes the system design in both hardware and recognition architecture to meet the system's goals. Figure 4a shows the overview of our recognition system, which consists of 4 main stages: reading the voltage signal, segmenting the signatures, extracting unique features, and recognition. We have employed 16 different features in both time and frequency domain, and make performance comparisons between two simple and light-weight classifiers Gaussian Mixture Models(GMM) and k-Nearest Neighbors (k-NN).The output of our device recognition can be expanded to some applications that we have mentioned: ATM Authentication, unlocking doors and turning on communications. Figure 4b shows the hardware architecture of inside mobile devices and the *on-top*, which consists of an amplifier module and microcontroller for processing data. The objective of designing amplifier is to enhance the signal strength and also to convert the bipolar to unipolar signal as we have mentioned. A small copper plate is placed in contact with the screen surface to capture the voltage signal. This contact copper forms the capacitances with both driving electrode (red dot) and sensing electrode (blue dot) inside mobile devices. The driving signal generated from touch controller charges and discharges the mutual capacitance C_M formed between driving electrodes and sensing electrodes for touch sensing purpose and, therefore, it also charges and discharges the capacitances between copper plates and electrodes, which is the source of the voltage signal we captured.

4. EVALUATION

Implementation: We have implemented the prototype which consists of Arduino Mini Pro 3.3V 8Mhz as microcontroller, bipolar to unipolar and amplifier module using LM324N IC. The figure 4c shows the top view of our prototype in triggering communication with Samsung Galaxy Note 10.1.

Preliminary Results: We present two evaluation results: (1) the recognition rate in all combination mobile devices, (2) the efficient power consumption of our method compared to BLE and NFC in triggering communication application. For the first experiment, we capture the voltage pattern emitted from mobile screen by placing the wearable device horizontally on the bottom left of the screen so that the 2x2cm copper plate is in contact with the screen surface.We then collect 20 samples/device from 14 mobile devices in total, which are from three different makers: Samsung(8), Apple(5) and HTC(1). Among these devices, there are 4 same model Galaxy S4, 3 same model Galaxy S5. A half of dataset is used for traning, the rest is for testing. The Table 1 shows that the *on-top* can achieve **100%** and **98.2%** recognition rate by using k-NN and GMM classifier, respectively. The feature Mel Frequency Cepstral Coefficents (MFCCs) and Root Mean Square (RMS) are chose in combination through sequential forward feature selection to obtain the best results. Second, we convince the power savings of *on-top* compared with BLE (BLE HM-10 [2]) and NFC (SM130 Mifare 13.56 MHz [3]) on the scanning state by using Monsoon power monitor 3.3V supply. We observed that our method, on average, only consumes **1.65mW** more than the Arduino baseline **(22.74mW)** while BLE and NFC module make these methods consume **30.16mW** and **63mW** more than Arduino alone. It means that our method consumes less **38.18x** power compared to NFC and **18.28x** power compared BLE. The response time for classifying one device is **153ms** and **9.2ms** by using k-NN and GMM, respectively.

Table 1: The performance of k-NN and GMM for all mobile devices.

Setup	Precision	Recall	F1-score	Selected Features
GMM	98.33	98.40	98.37	[MFCC, RMS]
kNN	100	100	100	[MFCC, RMS]

5. CONCLUSIONS AND REMARKS

In this work, we introduce *on-top*, a touchscreen mobile device identification technique that leverages the COTS capacitive screen signatures. While the preliminary results show the high recognition rates on the current mobile dataset with efficient power consumption in the scanning state compared to the traditional communication methods, we do realize that a much more extensive testing is needed to confirm our observation on the uniqueness of the capacitive signatures. We plan to recruit a large number of devices of different makers, models, and of the same batch for our evaluation. We also plan to explore more possible applications to make use of this technique.

6. REFERENCES

[1] G. Barrett and R. Omote. Projected-capacitive touch technology. *Information Display*, 2010.
[2] J. T. Company. Bluetooth 4.0 ble module, 2014.
[3] SONMICRO. Sm130 13.56 mhz rfid mifare module, 2008.
[4] G. Walker. Fundamentals of touch technologies and applications. *Society for Information Display*, 2011.
[5] T. Wang and T. Blankenship. Projected capacitive touch systems from the controller point of view. *Information Display*, 2011.