Demo: User Identification and Authentication with Capacitive Touch Communication

Tam Vu[†], Ashwin Ashok[†], Akash Baid[†], Marco Gruteser[†],
Richard Howard[†], Janne Lindqvist[†], Predrag Spasojevic[†], Jeffrey Walling[‡]
[†] WINLAB, Rutgers University, [‡] Dept. of Electrical and Computer Engineering,
{tamvu, aashok, baid, gruteser, reh, janne, spasojev}@winlab.rutgers.edu
{jeffrey.s.walling}@rutgers.edu

ABSTRACT

Today's identification and authentication mechanisms for touchscreen-enabled devices are cumbersome and do not support brief usage and device sharing. To address this challenge, this work explores a novel form of "wireless" communication that exploits the capacitive touchscreens which are now used in laptops, phones, and tablets, as a signal receiver. Using a custom built hardware token, in the form of a wearable ring, we show a proof-of-concept system that transmits a user identification code to the mobile device through the touchscreen. This mechanism works without any modification to the hardware or the firmware of the mobile device.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless Communication*

General Terms

Design, Measurement, Experimentation, Performance

Keywords

Signet Ring, Touchscreen Communication, User Identification, Capacitive Touchscreen

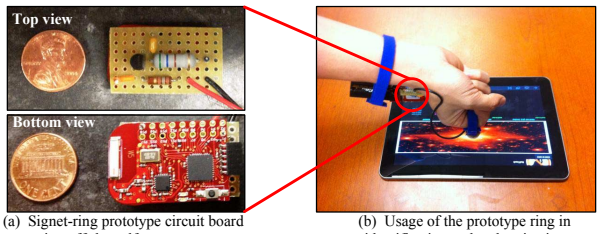
1. INTRODUCTION

Mobile devices provide us ubiquitous access to a vast array of media content and digital services, for example, access to our emails, photos, vehicle [4], house [1] and even accounting services such as bill-pay. As we increasingly rely on a variety of such mobile devices, we tend to quickly switch between them and temporarily share them with others [2]. We may let our children play games on our smartphones or share a tablet with colleagues or family members. Sometimes a device may be used by two or more people simultaneously, for example when playing a multi-player game. In all these situations, it would be of great benefit for the device to know who is interacting with it.

In this work, we show a proof-of-concept demonstration[1] of a novel form of "wireless" communication, that we term *capacitive touch communication* to address this challenge.

[1]Demo video is available at http://youtu.be/xmK1jH7iTuU

MobiSys'12, June 25–29, 2012, Low Wood Bay, Lake District, UK.
ACM 978-1-4503-1301-8/12/06.



(a) Signet-ring prototype circuit board using off-the-self components

(b) Usage of the prototype ring in identification and authentication

Figure 1: Ring Prototype

The key idea is to exploit the pervasive capacitive touchscreen and touchpad input devices as receivers to identify bit-strings being transmitted from transmitters embeded in wearable artifacts, such as a ring.

These hardware tokens transmit electrical signals when it comes in contact with the screen either directly or through the finger. This signal spoofs the effect of human touch on the screen and thus results in touch events being registered to the device's operating system. Our software inside the device uses the number and timing information of those registered events for demodulating the transmitted data.

2. DEMO

We will show a custom-built hardware token, as in Figure 1-a, controlled by a battery-powered microcontroller TI-MSP430F2722 [3] that is programmed to carry a user's identification in the form of a bit sequence. The microcontroller generates modulated 3 Volt square waves at a frequency of 1 KHz. We will show how the user's identification embedded on the ring hardware is demodulated by the tablet, a Samsung Galaxy Tab 10.1, from the artificial touch events triggered by the square waves.

We will also demonstrate the capability of indirect communication in enabling a novel technique to differentiate two users simultaneously interacting with the same touchscreen in a shared-screen two player game such as Fruit Ninja. The two users (only one of them wears the ring) will play the game on the same touchscreen and our receiver software will differentiate each of the users.

3. REFERENCES

[1] Craftsman. Assurelink garage doors openers. http://bit.ly/HJyH2V.
[2] A. K. Karlson, A. B. Brush, and S. Schechter. Can I borrow your phone?: understanding concerns when sharing mobile phones. In *Proc. of CHI*, Apr. 2009.
[3] Msp430 ultra-low power microcontrollers. http://msp430.com.
[4] E. Sofge. Can a smartphone make your car smarter? *MSN Autos*, 2010.