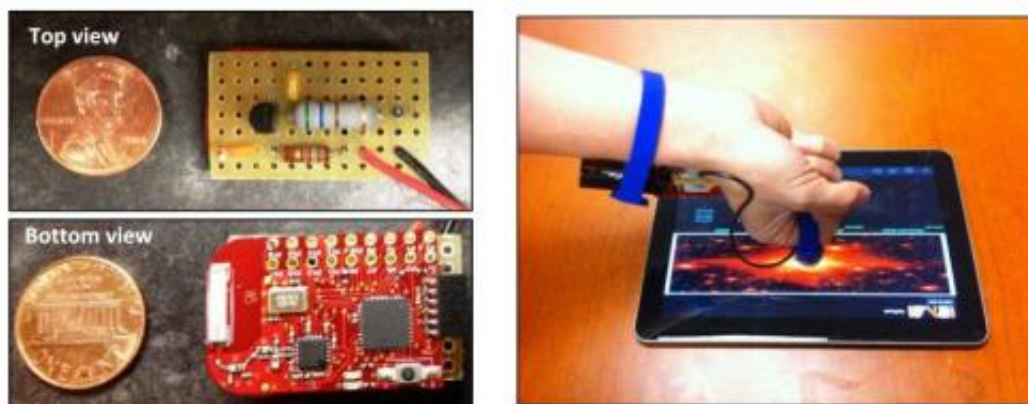


Rutgers team has ring prototype for touch authentication

August 31 2012, by Nancy Owano



The prototype ring and its usage for transmitting short messages from the ring to a touchpad. Image credit: Tam Vu

(Phys.org)—What about using the same mobile device touchscreens used every day for direct authentication? What if your touch alone identifies you by code from the ring on your finger? A team from the WINLAB at Rutgers University has turned the what-ifs into a device that makes use of capacitive touchscreens on phones and tablets to confirm the user's identity. The device can provide an additional layer of protection alongside passwords. The device can send a few bits of data representing a password from a special battery powered ring (with flash memory) on the finger. The data is sent as tiny voltage bursts through the wearer's skin for phone-screen capture.

Touchscreens are already designed to detect voltage changes from fingers touching and moving across the screen. They pick up those spikes, and software on the phone would read them as password-like data. Full details of their proposed approach can be seen in their research paper, "Distinguishing Users with Capacitive Touch Communication," by Tam Vu, Akash Baid, Simon Gao, Marco Gruteser, Richard Howard, Janne Lindqvist, Predrag Spasojevic, and Jeffrey Walling. "We explore a novel form of [wireless communication](#) in which a touch panel acts as a receiver and a small ring-like device worn by the user serves as the transmitter."

Project leader Marco Gruteser said the team hopes to commercialize the device in two years. Their homework ahead includes coming up with a miniaturized version of the device, as the one they have now is too "clunky." Also, the ring can transmit only a few bits of data per second quickly and accurately. "Our experiments show that this is feasible even with an off-the-shelf touchscreen system, albeit at very low bitrates," the authors wrote.

The equivalent of a pin code takes around two seconds for the ring to transmit, but Gruteser said that could be speeded up by modifying touchscreen [firmware](#) in phones. "We believe that significantly higher data rates could be achieved by designing receiver capabilities into touch screens," the authors wrote.

When the device is ready for prime time, their ring approach can be counted among the numerous attempts researchers are now making to provide easy but reliable authentication for mobile users. In expanding on that approach, as one computer scientist has suggested, research could lead to a time where numerous electronic devices are developed that "know" their users via touch and can adapt to preferences and offer personalized information.

As the authors point out, examples of "who you are" today include iris recognition, face recognition and voice recognition, all of which are being prototyped and tested on [mobile devices](#). With the advent of well known spoofing mechanisms, though, there is more work ahead. The authors point out that even novel approaches such as air gesture based [authentication](#) which uses accelerometer sensors of a mobile [device](#) are easily visible to an adversary and can be socially awkward.

A finger-swipe is something people are already doing, said Gruteser. The appeal of the approach is that so many devices use swiping already, whereas few commercial devices have retina-readers or finger-scanners.

WINLAB (Wireless Information Network Laboratory) at Rutgers, described as a cooperative industry-university research center, focuses on new ideas for the mobile Internet.

More information: [www.winlab.rutgers.edu/~grutes ...
/papers/tammob12.pdf](http://www.winlab.rutgers.edu/~grutes.../papers/tammob12.pdf)

via [Technology Review](#)

© 2012 Phys.org

Citation: Rutgers team has ring prototype for touch authentication (2012, August 31) retrieved 15 June 2024 from <https://phys.org/news/2012-08-rutgers-team-prototype-authentication.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.