Secure passwords can be sent through your body, instead of air

27 September 2016, by Jennifer Langston

UW engineers use a smartphone to send a secure password through the human body and open a door with an electronic smart lock. These “on body” transmissions employ low-frequency signals generated by the phone’s fingerprint sensor. Credit: Mark Stone/University of Washington

Sending a password or secret code over airborne radio waves like WiFi or Bluetooth means anyone can eavesdrop, making those transmissions vulnerable to hackers who can attempt to break the encrypted code.

Now, University of Washington computer scientists and electrical engineers have devised a way to send secure passwords through the human body—using benign, low-frequency transmissions generated by fingerprint sensors and touchpads on consumer devices.

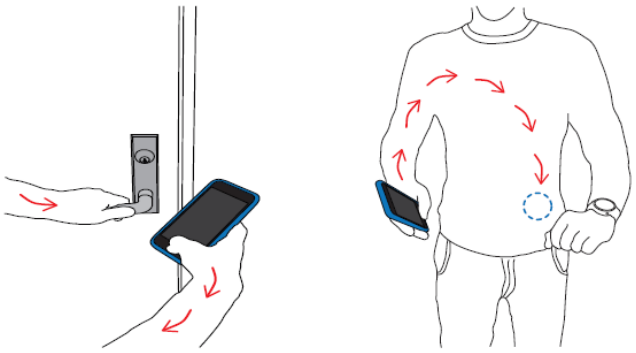
"Fingerprint sensors have so far been used as an input device. What is cool is that we've shown for the first time that fingerprint sensors can be re-purposed to send out information that is confined to the body," said senior author Shyam Gollakota, UW assistant professor of computer science and engineering.

These "on-body" transmissions offer a more secure way to transmit authenticating information between devices that touch parts of your body—such as a smart door lock or wearable medical device—and a phone or device that confirms your identity by asking you to type in a password.

This new technique, which leverages the signals already generated by fingerprint sensors on smartphones and laptop touchpads to transmit data in new ways, is described in a paper presented in September at the 2016 Association for Computing Machinery's International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2016) in Germany.

"Let's say I want to open a door using an electronic smart lock," said co-lead author Merhdad Hessar, a UW electrical engineering doctoral student. "I can touch the doorknob and touch the fingerprint sensor on my phone and transmit my secret credentials through my body to open the door, without leaking that personal information over the air."

The research team tested the technique on iPhone and other fingerprint sensors, as well as Lenovo laptop trackpads and the Adafruit capacitive touchpad. In tests with 10 different subjects, they were able to generate usable on-body transmissions on people of different heights, weights and body types. The system also worked when subjects were in motion—including while they walked and moved their arms.



(a) Authenticating door locks (b) Secret keys for wearables

Potential applications for on-body transmissions include securely sending information to door locks, glucose sensors or other wearable medical devices. Credit: Vikram Iyer, University of Washington

"We showed that it works in different postures like standing, sitting and sleeping," said co-lead author Vikram Iyer, a UW electrical engineering doctoral student. "We can also get a strong signal throughout your body. The receivers can be anywhere—on your leg, chest, hands—and still work."

The research team from the UW's Networks and Mobile Systems Lab systematically analyzed smartphone sensors to understand which of them generates low-frequency transmissions below 30 megahertz that travel well through the human body but don't propagate over the air.

The researchers found that fingerprint sensors and touchpads generate signals in the 2 to 10 megahertz range and employ capacitive coupling to sense where your finger is in space, and to identify the ridges and valleys that form unique fingerprint patterns.

Normally, sensors use these signals to receive input about your finger. But the UW engineers devised a way to use these signals as output that corresponds to data contained in a password or access code. When entered on a smartphone, data that authenticates your identity can travel securely through your body to a receiver embedded in a device that needs to confirm who you are.

Their process employs a sequence of finger scans to encode and transmit data. Performing a finger scan correlates to a 1-bit of digital data and not performing the scan correlates to a 0-bit.

The technology could also be useful for secure key transmissions to medical devices such as glucose monitors or insulin pumps, which seek to confirm someone's identity before sending or sharing data.

The team achieved bit rates of 50 bits per second on laptop touchpads and 25 bits per second with fingerprint sensors—fast enough to send a simple password or numerical code through the body and to a receiver within seconds.

This represents only a first step, the researchers say. Data can be transmitted through the body even faster if fingerprint sensor manufacturers provide more access to their software.

More information: Paper: onbody.cs.washington.edu/files/bodycomm.pdf

Provided by University of Washington