Cyber security Expert: Your Smartphone Will Soon ID You

Several parts of this new technology have been floating around for a couple of years, but now it has all congealed into a draconian nightmare: Your smartphone will, thanks to as many as a dozen on-board sensors, be able to ID you, just by being on your person. Thus, your identity could precede you like radar in reverse. TN Editor

The things that make human beings unique – fingerprints, irises, facial features – have become the preferred way to sign onto banking accounts online or other sensitive websites, the newest solution to the problem of hackable and forgettable passwords.

But your fingerprints can be stolen, your photo replicated. Now cyber experts are looking at the next security step: cellphones and computers that actually recognize you from a variety of factors.

Your smartphone now gathers more information about you than you probably realize.

"It's amazing how many sensors there are on a modern-day smartphone. You have motion sensors, like an accelerometer, a gyroscope and magnetometer," said John Whaley, chief executive of UnifyID, a start-up that offers what it calls revolutionary authentication.

Then you have other sensors, such as GPS, Bluetooth and Wi-Fi. All told, an average smartphone has 10 or so sensors measuring precise details about location and user habits.

"We can tell what floor of a building you're on. We can tell if you are inside or outside of a building," Whaley said. "Just with a few seconds of your walking data, from your phone sitting in your pocket, we can actually identify you based on that."

All told, smartphones can measure the angle that your cradle your devices, the pressure you put on the screen, how much of your finger touches the pad, the speed at which you type, how you swipe, your physical rhythms, the times you normally stir in the morning, some 100 or more indicators that in combination can give near total accuracy in identifying you.

"Once you combine a large number of these factors together, we can actually get to 99.999 percent accuracy about it being you versus not you," Whaley said. "At that threshold, you can actually use this for authentication and you don't have to use passwords anymore."

If passwords become a thing of the past, it is likely due to what computer scientists describe as machine learning – which allows computers to find hidden insights without being explicitly programmed where to look – as well as improvements in sensors that measure our lives and actions with precision. What Whaley calls "implicit authentication" may change the way humans interact not only with phones and websites, but maybe the world at large. ATMs may recognize us as we approach. Clerks or cash registers at stores may greet us by name as their computers recognize our smartphones.

Whaley, who has a master's degree in computer science from MIT and a doctorate in the field from Stanford, is catching attention. His company competed with scores of others as the most innovative start-up in the field of cybersecurity at the RSA conference in San Francisco last week, which drew 43,000 attendees, and won in a unanimous decision of the judges.

Technology to ensure authentication of users would have repercussions in banking and finance, e-commerce, cybersecurity, transportation security and in fraud detection, sectors with a value that nearly reaches $2 trillion.

“The need for extended authentication technology is going to be great,” said Robert Capps, vice president of business development at NuData Security, a Vancouver firm that uses behavioral analytics to help clients identify good users from bad ones.

The downside to using biometrics, such as fingerprints, in computer security is not widely understood.

Read full story here…