Could New Biometrics Finally Kill Smart Cards and Passwords?

A mix of sensors and AI, networks or buildings could soon know who you are without you having to tell them.

Kevin McCaney
Thu, 05/24/2018 - 10:04

Gaining access to a network or secure building has always been based on some combination of three things: something you know (usually a password), something you have (a smart card) and something you are (like a fingerprint). The next stage of authentication — toward a more secure, less aggravating process — lies in what you do and how you do it.

That’s what biometric companies, the Defense Department and other government agencies are aiming for, with a broad mix of biometrics and machine learning.
features that can be incorporated into smartphones and other devices to provide more seamless access for authorized users.

The idea of using motion sensors in authentication systems as a more effective, tamper-proof method than established techniques has been in the works for a while. And although plans to introduce wider use of them haven’t come along as quickly as first envisioned — DOD said two years ago, it planned to replace Common Access Cards with a biometric system by now — the addition of artificial intelligence and machine learning features is making behavioral biometrics even more viable. AI is improving face recognition to the point where people won’t have to stand still in front of a reader to be recognized. And the range of biometric authenticators — such as finger vibrations as opposed to prints, heat beats or ear prints — is expanding.

And like so many other things these days, it will be on your phone or a similar device. A Gartner report earlier this year projected that 80 percent of new commercial smartphones will have AI capabilities in 2020, compared with 10 percent in 2017. And because of that and other factors, Gartner predicted AI-powered behavioral biometrics would soon replace passwords and other current authentication factors.

**Biometric Plans in Motion**

DOD, for one, still plans to replace CACs with a system that combines traditional biometrics such as facial recognition, voice prints, and iris scanning with behavioral traits like device handling, a person’s gait, keystroke cadences and speech patterns. Together, they would provide what Steve Wallace, technical director at the Defense Information Systems Agency, recently described to Nextgov as a “risk score.”

Lt. Gen. Alan Lynn, then Defense Information Systems Agency director, called it an “identity score” last June at a cybersecurity symposium in Baltimore. By either name, the score would determine a user’s level of access to a network or building. DISA in January awarded Qualcomm a contract to develop “actionless authentication” using multiple factors.

There is, at first, a counterintuitive element to this new range of biometrics because of how they can change over time. One of the selling points for using irises, palms
or the trusty fingerprint is not only that they are unique to each individual, but also that they don’t change. They provide a constant point a reference to a person’s identity. Behavioral biometrics, on other hand, can evolve. A wrist injury could affect how someone handles a phone. A leg or back injury will change someone’s gait. Could those mutable features be as reliable as permanent ones?

Actually, yes. For one thing, the permanence of something like a fingerprint also is a potential weakness, as it could be stolen and/or compromised, which could have a lasting, even permanent, impact on a user. Behavioral biometrics, aided by AI and machine learning, could keep up with behavioral changes because authentication would be a continuous process.

It’s also noninvasive, collecting its data without input from the user, which would appeal to anyone — by which we mean everyone — who knows the aggravation of keeping track of a passel of passwords just to get through a day.

**Cutting the Cards**

DISA’s plan also would get rid of some of the problems the agency has with using CACs, which are trustworthy in many ways — carrying a photo, encrypted data and some biometric information — but aren’t always convenient. For soldiers in deployed environments, producing an ID card for access to, say, a command tent isn’t always practical. DISA’s system, which Wallace said is being developed by a contractor — also would be adaptable to different circumstances. It will maintain, say, 10 biometric identifiers but only use five at a time, allowing for different sets of factors being used for a secure area than for a public building.

If successful, biometric systems like the one DOD is planning are likely to catch on elsewhere in government. Civilian federal agencies have some complaints about Personal Identity Verification cards, for example, including the fact many smartphones people use aren’t covered by PIV’s protections.

Unlike two years ago, DISA hasn’t put a date on when its biometric system will make CACs obsolete. And predictions that “passwords are dead” have been made before. But with a combination of sensors and AI, networks or buildings could soon know who you are without you having to tell them.