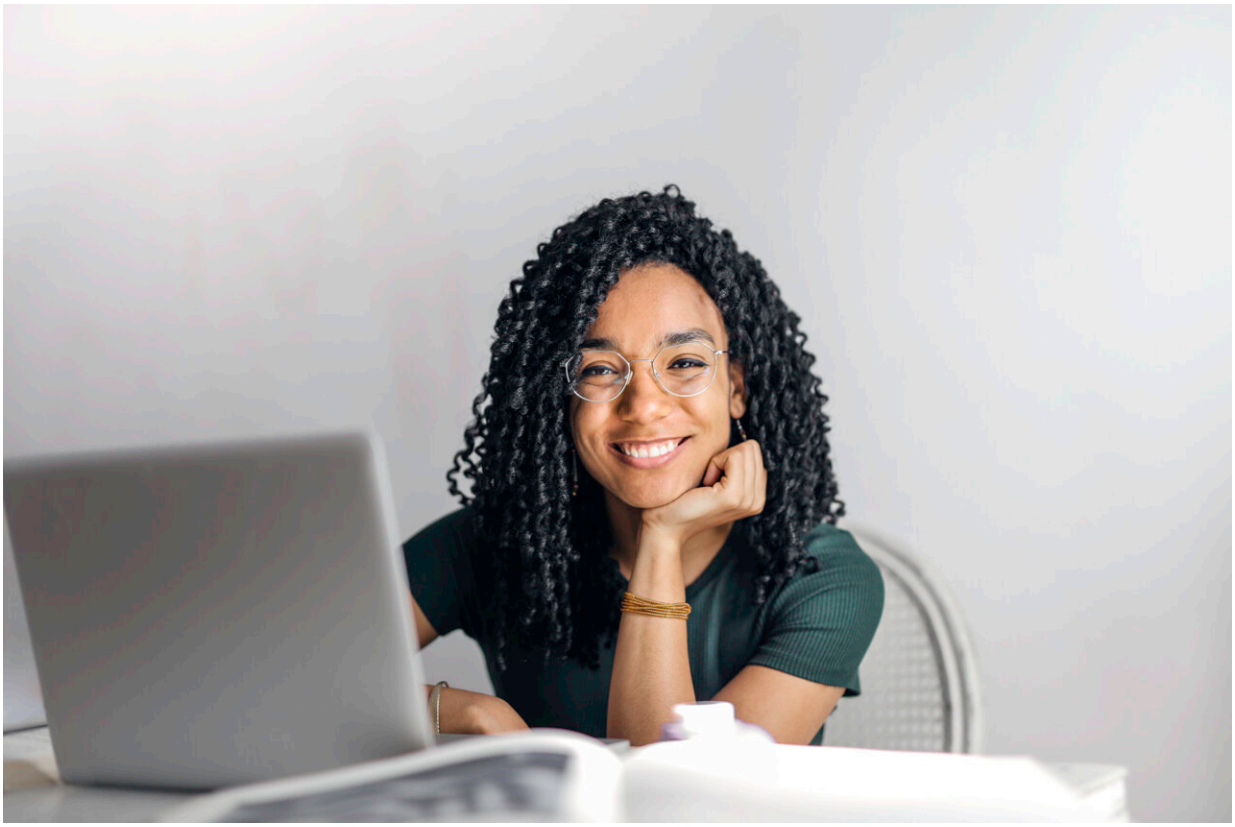
The challenge of authenticating real humans in a digital world

November 8 2017, by Jungwoo Ryoo



Credit: Andrea Piacquadio from Pexels

Proving identity is a routine part of modern daily life. Many people must show a driver's license to buy alcohol at a store, flash an ID card to security guards at work, enter passwords and passcodes to retrieve email

and other private information, and answer security validation questions when calling banks or credit card companies for customer service.

Authentication is also getting easier for people: Take the iPhone, for example. Unlocking the early versions required a multi-digit passcode. Then Apple introduced Touch ID, which would unlock the phone with a fingerprint reader. The latest version, just out, is the iPhone X, which can use its camera to perform facial recognition to authenticate a user.

As a software security researcher looking at authentication technologies for hand-held devices, I am fully aware that the technologies change, but the challenge remains the same: How can a digital system authenticate an analog human's identity?

Three factors of identity

There are three main ways of proving an identity. One involves something you know – like a password or your mother's maiden name. This method assumes the authorized user will have information no unauthorized user does. But that's not always the case: For 145.5 million Americans affected by the Equifax security breach revealed in September 2017, reams of previously private information may now be known to criminals.

A second method of authentication is with something you have – such as a key to your home's front door or a smart card to swipe at work. This assumes a limited number of people – possibly as few as one, but it could be a small group of users, like a family or co-workers – are allowed to enter a physical space or use a digital service.

A third way is by authenticating the individual human being – who you are – with some aspect of your biology. There are various type of these biometrics, such as fingerprints, facial recognition, iris scanning and

voiceprints. This strategy, of course, assumes that the bodily feature is unique to the particular individual – and, crucially, that the digital system involved can tell the difference between people.

Using two or more methods together can improve security and is called two-factor, or multi-factor, authentication.

The consequences of digital authentication

This increasing dependence on digital authentication may actually result in less security. While cameras, sensors and other devices can make authentication easier for people to accomplish, they carry their own weaknesses.

When a system seeks to authenticate an individual, it must compare the information the person is presenting – what they know, what they have or who they are – against a previously stored database of authorized users. As the Equifax security breach makes clear, those databases are themselves vulnerable to attack. Information stolen from there could be used somewhere else – for instance, to identify which bank a particular person uses and answer security questions when calling to transfer money. Or the database itself could be corrupted, altering information so an attacker would be able to fake his way into a physical space or system.

Another potential security threat inherent in biometrics in particular is that criminals don't need to guess a password, or force someone to reveal it: The simple presence of the victim – even at gunpoint – can supply the fingerprint or face to authenticate and unlock a system.

Future complications

As authentication becomes more complicated, using multiple factors and secure communications between sensors and databases, users become less willing to jump through all the hoops. So security managers try to make the process easier for them without weakening the protections. This commonly happens on websites that urge users to log in using their Facebook or Google accounts; those sites rely on the advanced security of the tech giants rather than creating their own authentication systems.

In one futuristic scenario, authentication could occur without a user even noticing: When you walk into a store, facial recognition could identify and authenticate you. Then, at checkout, you'd need only to scan your purchases and leave – the store will automatically charge the credit card of your choice. This isn't science fiction: Amazon has patented a system for doing exactly this in its Amazon Go cashier-less convenience stores.

This is possible in part because of the increasingly common practice of computer systems authenticating each other – so the store's system would recognize you, connect to the credit card company and authorize your purchase all on its own.

It may be more convenient, and even more secure, than a magnetic strip on a plastic card in your wallet. But the potential dangers will require much higher security for private information, particularly biometric data . A real identity still comes down to flesh and blood.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

https://phys.org/news/2017-11-authenticating-real-humans-digital-world.html