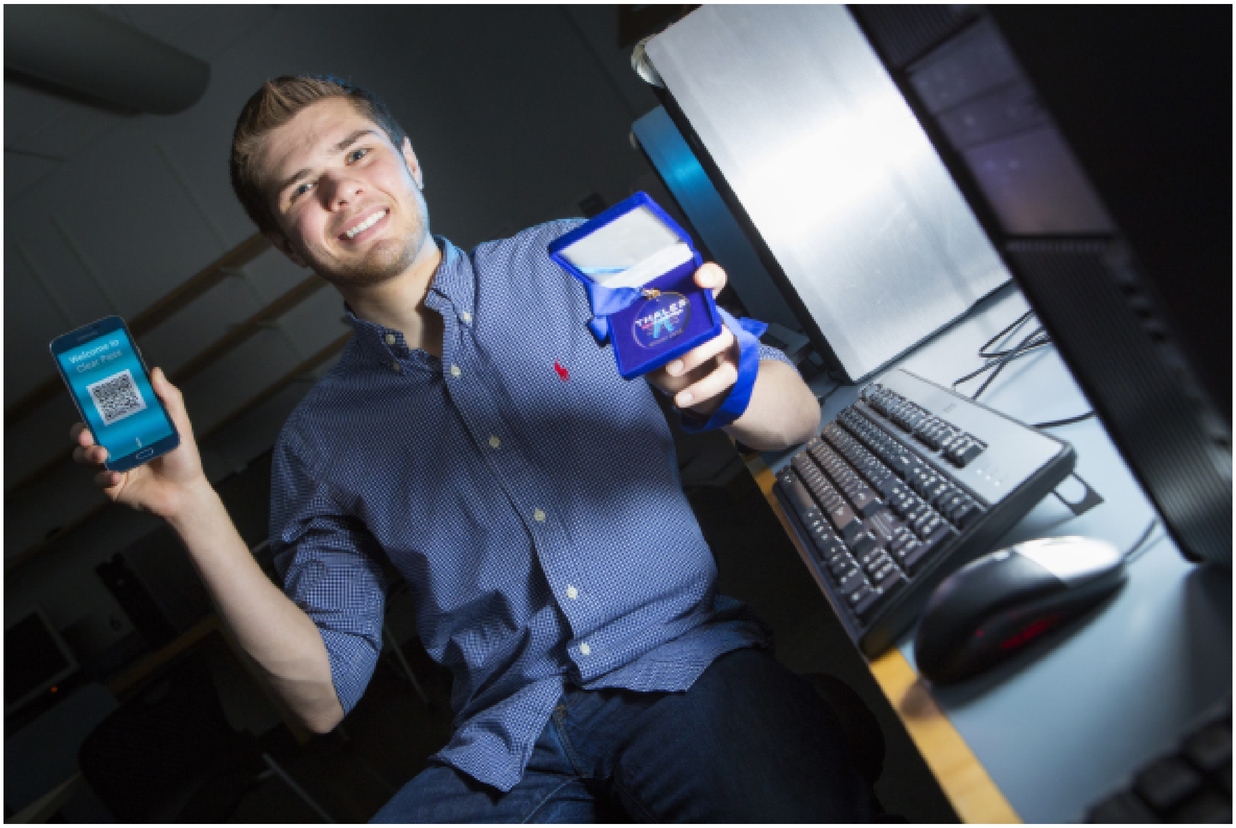
PHYS.ORG

Student develops fingerprint-based authentication app

March 3 2016



Nicholas Boucher, A.B. '19 (computer science), and a team of international students, developed a mobile app that seeks to enhance cybersecurity. Credit: Eliza Grinnell/SEAS Communications

Having trouble remembering all your online passwords? You're not alone. A recent study by identity management firm Centrify found that the average person has at least 19 online passwords, and that 25 percent of users forget at least one login detail each day.

With an eye toward improving cybersecurity, a Harvard John A. Paulson School of Engineering and Applied Sciences student developed a mobile app-based authentication system that enables users to log in to websites using a characteristic that is impossible to forget: their fingerprint.

Nicholas Boucher, A.B. '19, a computer science concentrator, and three teammates recently won the Cambridge University Hack-a-thon Cybersecurity Challenge for their app, ClearPass. "Hack Cambridge," the university's annual 24-hour coding marathon, was sponsored by British cybersecurity firm Thales.

"We thought that the concept of logging in with a username and password is pretty antiquated," Boucher said. "As a civilization, we ought to be able to move beyond that by now."

ClearPass exploits the biometric sensors on most smart phones to generate a unique user profile that an individual utilizes to log in to websites. A user scans his or her fingerprint, which the app uses to generate a secure QR code. Users hold the code in front of a computer's web cam to log in to a ClearPass-enabled website. Webmasters can enable ClearPass authentication by inserting into their sites just two lines of code, Boucher explained.

The app ensures security because no fingerprints are stored on the ClearPass server. Rather, ClearPass uses a hashing algorithm that scrambles and encodes fingerprint data. As an additional security feature, each QR code is only available for five minutes. As soon as it is used, the security token in the code is obliterated, making it useless for future login attempts.

"What makes ClearPass unique is that creating a username is optional," Boucher said. "It allows you to authenticate that you are who you say you are, all while maintaining full anonymity online."

Full anonymity could be especially useful when incorporated into a system like Bitcoin or certain banking and financial sites, Boucher said. And because the app works offline and is neither device- nor platform-specific, it could benefit a very broad user base.

For Boucher, one of the most exciting things about ClearPass is the potential to configure the system for any type of biometric data, such as facial mapping or vocal fingerprinting. ClearPass could even verify individuals using the heart rate sensor on a smart phone, effectively locking a user out of a site if he or she had an elevated pulse. If enabled, that feature could prevent a user from accessing a banking site if he or she were being forced to log in at gunpoint, Boucher said.

While heart rate scanning was one feature Boucher and his teammates weren't able to complete during the 24-hour Hack-a-Thon, he is looking forward to making further enhancements to the app.

"I think there could be some real uses for this," he said. "When you look at the broader possibilities of using biometric security for logging into everything from bank accounts, to ATMs, to Facebook, to email, with one swipe of a finger without changing any of your technology, the stakes become higher."

Provided by Harvard University

Citation: Student develops fingerprint-based authentication app (2016, March 3) retrieved 26 April 2024 from https://phys.org/news/2016-03-student-fingerprint-based-authentication-app.html