Non-Traditional Authentication Factors

Beyond the three traditional authentication factors, some experts have articulated additional "non-traditional" factors, including:

- *Where you are*: This factor involves assessing where a user is located based on information provided by the user's computer or mobile device.[1] Location-based information may be gleaned from Internet protocol (IP) addresses of computers or mobile devices, or may be provided directly by GPS (i.e., global positioning system) sensors contained in many mobile devices.[2]

- How you behave (or what you do): This factor—sometimes referred to as behavioral biometrics—involves identifying and analyzing the patterns of behavior of users (e.g., how they log in, navigate the website, move the mouse, or engage in transactions), and using these patterns to authenticate users in subsequent transactions.[3]

- *Somebody you know:* This factor involves having one or more third parties verify a user's identity (e.g., a financial or other institution).[4]

In a sense, these "non-traditional" factors may be viewed as extensions of the traditional authentication factors discussed above. Behavioral patterns, for example, may be viewed as a form of biometrics. A device that provides location-based information may be considered to be something that a user "has." Reliance on "somebody you know" may functionally mean "outsourcing" authentication to a third party that is itself relying on traditional authentication factors (as might be the case, for example, if a user is permitted to log on to a website using his or her Facebook or Google credentials). The use of various "non-traditional" factors, while not yet common, appears to be growing.

As concerns about security risks have grown, considerable attention has been paid to authentication issues. Indeed, in recent years, new approaches to authentication have been—and continue to be—tested, developed, and, in some cases, made commercially available. In early 2015, for example, the National Institute of Standards and Technology ("NIST") announced a competition for grants for "online identity verification systems that help improve the privacy, security and convenience of online transactions."[5]

ICIMutual
The safest decision you can make.

The text below is an excerpt from the ICI Mutual risk management study *Shareholder Authentication: Managing the Risk of Fraudulent Transactions.* The full study may be accessed at www.icimutual.com/ShareholderAuthentication.

Innovative New Approaches to Authentication

Geographical boundaries: One approach to location-based authentication, now under development, would require a user to select a place on Earth and to draw a boundary around it. The system would then create a password derived from the location (e.g., its latitude, longitude, and altitude) and the size and shape of the boundary. The approach assumes that the location and boundary would be relatively easy for a user to remember, but that the derived password would be difficult to crack.[6]

Behavioral biometrics: Some companies are seeking to develop "behavioral biometrics" software, which is based on the assumption that a user's behavioral patterns are predictable and sufficiently unique as to be used for authentication purposes.[7] One software program analyzes a user's typing patterns, including rhythm, speed, and length of a key press.[8] Another company's software (reportedly used by a large foreign bank) analyzes how a user utilizes his or her mobile devices—including how the screen is pinched, the angle at which a device is held, the pauses between letters while typing, and the pressureexerted on the screen. The software flags user behavior that deviates from the expected behavior based on the user's previous interactions.[9]

Endnotes

[1] *See* Sung Choi and David Zage, Addressing Insider Threat using "Where You Are" as Fourth Factor Authentication (undated), https://www.cs.purdue.edu/homes/zagedj/docs/iccst2012.pdf.

[2] *See* Jasper Hamill, *Future Apple gumble could lock fanbois out of their own devices*, THE REGISTER (July 3, 2014), http://www.theregister.co.uk/2014/07/03/apple_location_security_tech_could_auto_lock_your_istuff/.

[3] *See* Bob Forbes, *The Fifth Factor: Behavior Profiling Opens New Possibilities for Web Access Control*, DATA SECURITY MANAGEMENT (Apr. 2002), http://www.ittoday.info/AIMS/DSM/83-10-34.pdf.

[4] *See* SEC & Dep't of the Treasury, Joint Final Rule: Customer Identification Programs for Mutual Funds, Release No. IC-26031 & RIN 1506-AA33 (May 2003), *available at* http://www.sec.gov/rules/final/ic-26031.htm.

[5] *See* NIST, NIST Announces Pilot Grants Competition to Improve Security and Privacy of Online Identity Verification Systems (Feb. 12, 2015), http://www.nist.gov/itl/20150212_nstic_grants.cfm.

[6] *See* Richard Chirgwin, *New password system lets planet Earth do the hard work: Think of a place, any place…*, THE REGISTER (Feb. 17, 2014), http://www.theregister.co.uk/2014/02/17/new_password_system_lets_planet_earth_do_the_hard_work/.

[7] Paul Marks, *Forget passwords – to log in, just start typing*, New Scientist (June 27, 2014), http://www.newscientist.com/article/mg22229754.500-forget-passwords--to-log-in-just-start-typing.html.

[8] *See* Orr Hirschauge, *Beyond Passwords, Behavior Looms*, THE WALL STREET JOURNAL (July 11, 2014), http://online.wsj.com/articles/beyond-passwords-behavior-looms-1405084188.

[9] *See id.*

Information current as of September 2015