In our personal lives, we use several senses to identify or “authenticate” others: sight, hearing, and touch all play a role in recognizing someone, and we’re flexible enough that if only some of our senses detect an individual’s familiar characteristics, we still feel confident about that person’s identity. Furthermore, we draw on several aspects of each sense. For example, on the phone, we often recognize not only language and tone, but also intonation, diction, and other audible aspects that make the person on the other end identifiable to us. Even if it’s been years since we last saw or spoke with someone, our senses usually help us recognize them. We can decide how certain we are of their identity—saying hello doesn’t require the same level of trust as providing our Facebook login information.

Unlike humans, today’s computer systems don’t have the ability to recognize people. In early computing, most security was through physical access control such as a locked door. Authentication’s initial purpose was to track who was being charged for storage and computing time. However, the security environment has changed. Most computer access today permits sophisticated access control to one or more systems transparently, often relying on strong user authentication at the beginning of the session. This is a static mode of authentication; it’s typically performed using a token such as a password, smartcard, or biometric, or a combination of these methods to allow access to the information or services.

Although we have strong static authentication mechanisms, the interconnection of multiple systems makes the protection and management of data more important than ever. Strong authentication systems aren’t useful unless access is vigilantly protected. One concern with access control is when a user leaves the computer interface without logging off, or user abandonment. Simple methods of detecting user abandonment can create almost as many

Expanding Continuous Authentication with Mobile Devices

Kim B. Schaffer, National Institute of Standards and Technology

More sophisticated methods of detecting user interaction with computers and smartphones are needed for better security and usability. Multimodal continuous authentication is one of the more promising authentication methods on the horizon.
problems for the user as they solve. More sophisticated methods of detecting user interaction are needed for better security and usability.

ABANDONMENT ISSUES
Ideally, once a computer has authenticated a user, it becomes the user’s responsibility to protect access to the computer’s data. This is usually ensured by maintaining control over the user interface—no one else has access to that session. However, users can be forgetful or assume that no one else would use the computer while they run a quick errand. This problem is pervasive enough that system administrators usually enforce some form of user abandonment detection to prevent unauthorized access.

A common method of detecting user abandonment is to monitor the input devices. When there’s no user interaction after a preset time, the user is logged off either directly or through a screen saver. Although this method works well for many users, it can be frustrating if a user is reading, giving a presentation, or otherwise passively engaging with the computer. The prompt for the user to re-authenticate could distract the user (and others) or interfere with the user’s work. This method also carries the risk of the user’s authentication token being compromised if the authentication occurs in a public setting, such as a conference.

Unfortunately, monitoring for activity doesn’t determine whether a different user accesses the computer. Walking away for a moment leaves plenty of time for another user to take over the session. The new user has the same rights as the individual who logged in, including sending, deleting, and changing information. This is often easily accomplished without the original user’s knowledge.

Developing stronger methods of authentication and tighter policies doesn’t necessarily help the user maintain control. For example, smartcard policies often require that an authenticated smartcard remain in the card reader, tying the user to the system. However, in practice, the user is apt to walk away and leave the smartcard in the card reader. Because the smartcard might also be used for building access, the user could leave the area and not realize the smartcard is missing until trying to return, leaving the computer accessible to others in the area. Other policies could result in constraining the user to one device at a time. Although most office workers might not have a problem with this policy, those working in a lab environment often operate multiple machines simultaneously.

CONTINUOUS AUTHENTICATION
Continuous authentication offers a better alternative for monitoring user activity, with user confirmation based on behavioral biometrics. Behavioral biometric modalities continuously accumulate sensor information and correlate patterns of user activity, whereas with biometrics such as fingerprint determination used in static authentication, a sample is taken and analyzed and a one-time determination is made. Fingerprint modalities are also difficult to use as continuous biometrics because computer interfaces typically don’t maintain constant contact with a specific finger while the user interacts with the system. Continuous authentication takes advantage of available sensors and human interfaces through video, audio, or tactile devices such as keyboards or mice. By identifying a change in the user’s behavior, continuous authentication can detect whether the user abandons the session or whether someone attempts to pose as the user.

Current continuous authentication methods being studied or in limited use include analysis of the face, iris, and retina; body movements; voice and speech; and keyboard, mouse, touchscreen, and handwriting. Concerns with each of these include collection times, liveness detection, secure storage, and transmittals. Liveness detection is typically specific to the biometric being used. The April 2015 issue of IEEE Transactions on Information Forensics and Security offers a good selection of papers covering tactile, facial, and vocal modalities; their weaknesses; and possible countermeasures.

Platforms for continuous authentication
Part of the challenge of using continuous authentication in the workplace is the introduction of sensors. Working environments often restrict the insertion and use of sensors like cameras and microphones due to cost or security issues. In addition, newer technologies often present challenges as they are integrated into the workplace. For example, when the USB port was first introduced, organizations often considered it a recipe for compromise: small, easily hidden devices that can be used to steal a great deal of information or deliver malware.
Replacing static authentication with continuous authentication as the primary means of logging into a computer system could signal the end of unmonitored systems and passwords.

Touch-sensitive interfaces. Tablets and smartphones are beginning to be accepted in the work environment, often at the insistence of employees using their privately owned devices or in response to the increasing popularity of mobile work platforms. The sensors integrated into these platforms could help provide the additional resources needed for continuous authentication. Much of the recent research in continuous authentication is making use of smartphones and other mobile devices as they are viewed as devices being introduced into the workplace.

Implementation concerns
Adopting continuous authentication has been difficult. Behavioral biometrics have been around for some time, but a major obstacle is low processing power. However, the development of low-power multicore processing supports continuous authentication schemes without handicapping the user, and the increased processing efficiency embedded in many mobile devices can now simultaneously support sensor acquisition, assessment, and the user.

Another issue is the handling of biometric data. At some level, behavioral biometric data needs to be tightly connected to identity management. A logical place for the association and collection of biometric data might be under the entity responsible for identity management. It might be possible to disconnect the association at the systems level, providing biometric information as needed without the direct association with the user’s identity. However, biometric information might have to be shared with each system performing continuous authentication. As biometric data collection matures, it’s likely to become more compact and secure. However, access from other systems—including modification or substitution of biometric templates—is a major concern to the identity manager, authentication system administrator, and end user. Privacy will remain a critical issue for all authentication mechanisms until it’s adequately addressed.

Although specific biometric modalities can be applied to most individuals, a small but important segment of the population—such as those with physical limitations—can’t be monitored due to an inability to obtain user measurements for a particular modality. Ubiquity is more easily achieved by combining different modes of biometrics. Multimodal biometrics combine two or more biometric modalities to alleviate some of the limitations that can result from a single modality. This fusion makes continuous authentication feasible in today’s market and is necessary to offset the limitations of individual authentication methods due to user nonuniformity. It might even be possible to identify a user by the lack of information, such as when, due to a limitation, a user provides voice-to-text input rather than keyboard input. Multimodal biometrics could also make compromising a user more difficult if each biometric signature is protected separately.

Replacing static authentication with continuous authentication as the primary means of logging into a computer system could signal the end of unmonitored systems and possibly the end of passwords. For much of its development, continuous authentication has been used as a stand-alone service. By linking continuous authentication with identity management, an organization has authoritative knowledge of the user, binding the biometrics to user identity. The primary issue in replacing static authentication is that many continuous authentication modalities have difficulty identifying users quickly and with a high degree of confidence. However, merging behavioral authentication modalities—especially by including audio or video behavioral biometrics—could enable the system to monitor the user for a sufficient period of time prior to logging in, making the authentication appear instantaneous.

Encouraging continuous authentication
Mobile devices might be the best platform for early continuous authentication. Multiple sensors are already available for robust continuous authentication integration. In addition, mobile device manufacturers are trying to attract users by creating features that are unique to their devices. If biometric data and processing can be done within the device, the user will have physical control of the private biometric template and processing, thereby reducing some risk. Once the technology is successfully implemented, the user will be able to use the device in a public area with little fear of authentication information being compromised.

For large systems, it might be possible to support multiple users in the same session, whereas mobile devices...
could be more limited. Continuous monitoring can bring the user closer to the system; as long as the user is interacting with the system, the user is in control. However, it can’t allow the user to maintain an active session while not interacting with the system, such as when a system administrator is doing a configuration for the user. With continuous authentication, as soon as the user stops using the computer or another user sits down at the computer, the computer should lock. The user temporarily surrenders control and suspends the continuous monitoring so that work can be done by others as needed. Although several options can be pursued, allowing the user to suspend monitoring for a given time might be appropriate.

Unlike static authentication, multimodal continuous authentication must aggregate the response of each mode as it becomes available. It might be possible to take advantage of varying confidence during early or unsatisfactory periods of monitoring authentication to allow the user to access services or data that aren’t sensitive in nature. For example, at the start of each session, the authentication is likely degraded due to lack of sampling data. However, this might be a good time for verifying patch management, checking the weather, or other similar low-threat services. User accidents or other changes must also be addressed: accidents that result in changes to monitored features or neurological impacts could force users to re-enroll. With a multimodal system, the reduction or loss of one type of monitoring doesn’t prohibit use of the system.

Multimodal continuous authentication is one of the more promising authentication methods on the horizon. The additional resources and sensors in today’s mobile products appear to support continuous authentication methods over static authentication methods that are often difficult to deploy and manage in terms of cost and security. As systems begin to support continuous authentication, users might feel less pressure to memorize or carry their login credentials, and system managers might feel more confident of the identity of those using their accounts.

REFERENCES

KIM B. SCHAFFER is an IT specialist in security at the National Institute of Standards and Technology. Contact him at kim.schaffer@nist.gov.