Mobile Devices expand Continuous Authentication

In our personal lives we use several senses to identify or *validate* someone. We can acknowledge someone without checking their credentials each time. Sight, hearing and touch may all play a part of us "authenticating" others, and we're flexible enough that if only some of our senses detect things that we are familiar with, we may still feel confident as to the identity of an individual. Furthermore, there are several aspects of each sense that we can draw on; for example, over the phone we often recognize not just language and tone, but also intonation, diction and other audible aspects that make the person identifiable to us. Drawing on several of our senses, we may be reasonably certain who a person is before they speak to us, possibly even though it has been years since our last meeting. And we can decide how certain we need to be for that interaction. Saying hello doesn't need the same level of trust as giving them our Facebook login information.

While we have these incredible abilities to recognize people, today's computer systems do not. In early computing, most of the security was by physical access control. The initial purpose of authentication was to find who was charged for storage and computing time. However, the 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 one-time authentication at the beginning of a session is often referred to as a static mode of authentication [1]. Static authentication is typically performed using some sort of token such as a password, smart card, biometric or a combination of those methods to give access to the information or services needed.

While we have strong static authentication mechanisms, access to the information through the interconnection of multiple systems makes the protection and management of the data more important than ever before. Strong authentication systems are not useful unless the user is also vigilant in protecting access to the information. A concern with access control is the user being drawn away from the computer interface without logging off. Simple methods of detecting user abandonment create almost as many problems for the user as they solve. More sophisticated methods of detecting user interaction are needed for better security and usability. Some of the limitations of managing the user access need to be reevaluated as to the risk they permit.

Abandonment issues

Ideally, once the user is authenticated it becomes their responsibility to protect access to the data. This is usually ensured by maintaining control over the user interface, i.e. no one else uses that session. However, users are sometimes forgetful or trust 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 aid in preventing unauthorized access.

A common method of detecting abandonment is to monitor the input devices. When there is no user interaction after a preset time, the operator is logged off either directly or through a screen saver. While this usability aid normally works well for many users, it can lead to a great deal of user frustration if they are reading, giving a presentation or involved in other passive uses of the computer. Unfortunately, the user's need to re-authenticate to continue may interfere with or distract the user (and others), by

focusing on producing the credentials, rather than the task at hand. It may also aid in the compromise of user's authentication token if it takes place in a public setting such as a conference.

Monitoring for activity unfortunately does not determine if another user is accessing the computer. Walking away for a quick errand often leaves plenty of time for another operator to take over the session. The new user has the same rights as the individual logged in, including sending, deleting and changing any information. And often this can be easily accomplished without the user's knowledge.

Using stronger methods of authentication and tighter policies do not necessarily aid in user maintaining control; smart cards policies often require an authenticated smartcard remain in the card reader tying the user to the system. However, in practice the user is apt to walk off and leave the smartcard in the card reader. Since the smartcard may also be used for building access, the user may leave the area and not notice the lack of the smartcard until trying to return, also leaving the computer accessible to those in the area. Other issues with a strong policy may result in constraining the user to one device at a time. While most office workers may not have an problem with this policy, a user working in a lab environment often finds it is necessary to operate multiple machines at the same time. Better methods are needed that improve both security and usability.

Defining continuous authentication

Continuous authentication attempts to offer a better alternative for monitoring the user's activity, with user confirmation based on behavioral biometrics [2]. Behavioral biometric modalities continuously accumulate sensor information and correlate patterns of user activity on an ongoing basis; whereas, biometrics such as fingerprint determination used in static authentication, takes a sample, analyzes it and a one-time determination is made. Fingerprint modalities are also difficult to use as continuous biometrics since computer interfaces typically do not maintain constant contact with a specific finger while the user interacts with the system. Continuous authentication tries to take 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 detects if the user abandons the session or if someone attempts to pose as the user.

Current continuous authentication methods under study or in limited use include analysis of face, iris and retina, body movements, voice and speech, keyboard, mouse, touch screen or hand writing. Concerns with each of these include collection times, liveness detection, secure storage and transmittals. Liveness detection is typically specific to the biometric being used. A good selection of papers covering tactile, facial and vocal modalities, their weaknesses and possible countermeasures can be found in the April 2015 issue of IEEE Transactions on Information Forensics and Security [3].

Platforms for Continuous Authentication

Part of the challenge of inserting 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. Newer technologies often present challenges as they are integrated into the workplace. As an example, when the USB port was first introduced, organizations often considered it to be a recipe for compromise. While the risk factors have not changed, many organizations consider USB ports to be useful; adding policies to mitigate risks. Similarly, technology that include cameras, microphones, GPS and wireless connectivity such as those in mobile devices may

present unevaluated risks to corporate environments. However these same services identified as having risks may also be part of more secure implementations of continuous authentication.

Mobile platforms are typically focused toward the individual and often include integrated microphones, cameras and touch-sensitive interfaces. Mobile devices such as tablets and smartphones are beginning to be accepted into the work environment, often by the insistence of the employees using their privately owned devices, or by demanding mobile work platforms. The sensors integrated into these platforms open opportunities for continuous authentication. These sensors may help provide the additional resources needed for continuous authentication. Much of the recent research is making use of smartphones and other mobile devices as they are viewed as devices being introduced into the workplace [4]. These mobile devices are also aiding continuous authentication in other ways.

Continuous Authentication Implementation Concerns

Adoption of continuous authentication has been difficult. Even behavioral biometrics have been around for some time. A major obstacle preventing adoption is processing power. Since the user expects the majority of the processing power to be available for use, the processing power required for the continuing authentication has not been available. The development of low power multi-core processing supports the development of continuous authentication schemes without handicapping the user. The increased processing efficiency embedded in many mobile devices can now support sensor acquisition, assessment and the user simultaneously.

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 might be under the entity responsible for identity management. It may 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 may have to be shared with each system performing continuous authentication. As biometric data collection matures, it is 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 to the end-user [5]. Privacy will remain a critical issue for all authentication mechanisms until adequately addressed.

While specific biometric modalities can be applied to a large portion of those to be monitored, a small, but important segment of the population cannot be monitored due to an inability to obtain user measurements for a particular modality. Ubiquity is more easily achieved by being able to combine different modes of biometrics. Multimodal biometrics combine two or more biometric modalities to alleviate some of the limitations that may be a result of a single modality [6]. It is this fusion of the different types of behavioral biometrics that make continuous authentication feasible in today's market from the population standpoint. Fusion is necessary to offset the limitations of individual authentication methods due to the non-uniformity of the users. It may even be possible to identify a user by the lack of information, such as keyboard input when voice-to-text input methods are used due to a user limitation. Multi-modal biometrics could also increase the difficulty of compromising a user if each biometric signature is protected separately.

The replacement or subsumption of static authentication to continuous authentication as the primary means of logging onto a computer system could mean the end of unmonitored systems and possibly the

end of passwords. For much of the development of continuous authentication, it has been used as a standalone service. By linking continuous authentication with identity management, the organization has authoritative knowledge of the user, binding the biometrics to user identity. The primary difficultly in replacement of static authentication is that many of the continuous authentication modalities have difficulties in quickly identifying users with a high degree of confidence. However, the merging of behavioral authentication modalities, especially by including audio or video behavioral biometrics may enable the system to monitor the user for a sufficient period of time prior to logging in, making it appear instantaneous.

Encouraging Continuous Authentication

Mobile devices may be our best platform for early continuous authentication. Multiple sensors are available for robust continuous authentication integration. Mobile manufacturers are trying to attract users by creating features which are unique to their devices. If the biometrics data and processing can be done within the device, the user will have physical control of the private biometric template and processing reducing some risk. Once 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 may be possible to support multiple users in the same session, whereas mobile devices may be more limited. Continuous monitoring can tie the user more closely to the system, as long as the user is interacting with the system, the user is in control. What continuous monitoring can't do is when the user wants to maintain an active session while the user is not interacting with the system, such as when a system administrator is doing configuration for the user. With continuous authentication, as soon the user gives up the computer or another user sits down to the computer, the computer should lock. The intention of the user is to temporarily surrender control and suspend the continuous monitoring so that needed work can be done by others in a better position to do so. While there are several options that can be pursued, it appears that 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 may be possible to take advantage of the varying confidence during early or unsatisfactory periods of monitoring authentication to allow the user access to services or data which are not 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 things like verification of patch management, checking weather or similar low threat services. User accidents or other changes to users may also be an issue that must be addressed. Accidents that result in changes to monitored features or neurological impacts may force users to have to re-enroll. By using multi-modal systems, the reduction or loss in one type of monitoring does not prohibit use of the system.

Summary

Multimodal Continuous Authentication appears to be one of the more promising authentication methods on the horizon. The additional resources and sensors in today's mobile products appear to support considering continuous authentication methods over mature static authentication methods that are often difficult to deploy and manage in terms of both cost and security. As systems begin to support continuous authentication, users may feel less pressure to memorize or carry the necessary credentials while system managers feel more confident as to who is using the user's account.

References

[1] T. Mustafi'c, A. Messerman, S. A. Camtepe, A.-D. Schmidt, and S. Albayrak, "Behavioral biometrics for persistent single sign-on," in *Proceedings of the 7th ACM workshop on Digital identity management*, 2011, pp. 73–82.

[2] H. Saevanee and P. Bhatarakosol, "User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device," in *Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on*, 2008, pp. 82–86.

[3] N. Evans, S. Z. Li, S. Marcel, and A. Ross, "Guest Editorial: Special Issue on Biometric Spoofing and Countermeasures," *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 4, pp. 699–702, 2015.

[4] K. I. Shin, J. S. Park, J. Y. Lee, and J. H. Park, "Design and implementation of improved authentication system for Android smartphone users," in *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, 2012, pp. 704–707.

[5] E. Martiri, "A State-of-the-Art on Continuous Authentication," *Mediterranean Journal of Social Sciences*, vol. 6, no. 2, p. 526, 2015.

[6] A. K. Nag, D. Dasgupta, and K. Deb, "An Adaptive Approach for Active Multi-Factor Authentication," in *9th Annual Symposium on Information Assurance (ASIA'14)*, 2014, p. 39.