Behavioral Biometrics for Universal Access and Authentication

Liam M. Mayron(✉)

Arizona State University, Tempe, AZ 85281, USA
lmayron@asu.edu

Abstract. Behavioral biometrics, such as gait, voice, handwriting, and keystroke dynamics can provide a method of authenticating users that is both secure and usable, particularly on mobile devices. Behavioral biometrics can often be collected in the background, without requiring a specific security task to be completed by the user. Many behavioral biometrics can be recorded with hardware that has already been deployed in many mobile devices. In this paper, we consider the use of behavioral biometrics for authentication in systems designed for universal access. Requirements for security and authentication are discussed, and several behavioral biometrics are introduced. Considerations for universal access are presented.

Keywords: Biometrics · Behavioral biometrics · Security · Usability · Authentication

1 Introduction

Universal access has as its objective to provide access to information technology to as broad a range of people as possible [29]. Although universal access is a notable goal, it is important to keep security considerations in mind as we design such systems [2]. This work seeks to emphasize one of the security-related aspects of universal access – authentication.

Users can be authenticated in several ways. Typically, this is done using either one or a combination of something a user knows, possesses, and is (biometrics). Although something a user knows may be forgotten, and something a user possesses may be lost, biometrics are tightly associated with the individual and cannot be left behind, making them an appealing option for a system that is secure, usable, and universally accessible [3,7,8,19,26,27].

There are many types of biometrics, each with their own benefits and disadvantages. Physical biometrics include fingerprint, face, and iris recognition. Fingerprints are widely accepted and considered to be a reasonably usable option [1,30], although face recognition can be done without requiring direct contact between the user and the sensor.

Behavioral biometrics are a versatile method of collecting information about and, potentially, authenticating users. These biometrics include patterns of

M. Antona and C. Stephanidis (Eds.): UAHCI 2015, Part I, LNCS 9175, pp. 330–339, 2015.
DOI: 10.1007/978-3-319-20678-3_32

human behavior, including their gait, voice, handwriting, and keyboard typing patterns. In contrast to certain physical biometrics, many behavioral biometrics can be collected with common and inexpensive hardware. Behavioral biometrics do not necessarily require physical contact for collection and can often be collected without the user's awareness of the activity. This passive collection makes behavioral biometrics and intriguing option for securing systems in an accessible manner.

Today, behavioral biometrics deployed are more frequently, particularly for purposes of authentication and security. Additional information, such as the context within which the desired action is occurring within, may also be used to strengthen a user's case for access to protected resources. Whereas traditional passwords are cumbersome on a small mobile device's touch screen, and physical biometrics hardware (such as fingerprint readers) remains a premium feature, it may be tempting to employ behavioral biometrics to protect and restrict access to resources.

This paper examines the potential and challenges facing the widespread use of behavioral biometrics for authentication, particularly as it relates to universal access. We will introduce behavioral biometrics, discuss requirements for effectively realizing such schemes, and consider impediments to the universal use of behavioral biometrics.

This paper is organized as follows: Sect. 2 introduces key concepts in security. Authentication is discussed in Sect. 3. Behavioral biometrics are detailed in Sect. 4. Finally, discussion and concluding thoughts are shared in Sect. 5.

2 Security

It is challenging to separate *universal* access from *secure* access. If the objective is to provide access to as broad a range of individuals as possible, as is the case with systems designed for universal access, we must also seek to provide access in a secure manner, for all users. Furthermore, just as new features or capabilities should not degrade the usability for any individual or group of users, the purposeful incorporation of universal access should not degrade the security experience for other users. There is tension between the security and usability of a system [22].

Security serves as a barrier to a system's resources, whereas universal access seeks to provide multiple methods of use. Additionally, it is often the case that systems that must prioritize universal access also provide access to some of our most sensitive personal and health-related information [2].

Broadly, a secure digital system must provide confidentiality, integrity, and availability [14,24].

- Confidentiality: a system must only provide access to users who are authorized to view a certain resource.
- Integrity: only the intended parties should be able to modify the information contained within the system.
- Availability: the system must not deny access to legitimate users.

Thus, we have the challenge of designing systems that must provide access to a wide range of individuals, but in a secure way.

In some cases, systems have a primary method of authenticating, with one or more alternatives provided for users who are not able to use the primary method. For example, a user who cannot use a fingerprint reader may be able to present an identification card instead. System designers should be wary, however, as this opens a system's authentication mechanisms to potential abuse. It can be easier to forge an identification card than a fingerprint. Indeed, abusers may purposefully damage or circumvent the primary authentication mechanism in order to gain access using a less secure, alternative way.

One example is a version of Google's ReCaptcha authentication system [32]. ReCaptcha authenticates users as humans (as opposed to automated robots) by asking them to identify the text in an image. The intention is that the text in an image is easy (or at least, easier) for a human to understand and challenging for a computer to decipher. An alternative mode of access was provided for those who had difficulty with the visual cue – audio would play instead. However, audio CAPTCHAs have been shown to be vulnerable to automatic deciphering – perhaps even more vulnerable than text-based CAPTCHAs [6]. Instead of using a wide variety methods of authentication, our objective should be fewer, but more robust and well-test methods capable of authenticating a wide range of individuals.

3 Authentication

Authentication can be defined in terms of the states before and after authentication has occurred. After authentication, two entities (users, computers, or other systems) should be confident that they are communicating with one another [5]. In terms of universal access to information technology, we will focus on authentication of the user to the system (although the converse remains an interesting topic – how does the user know they are connected to the intended endpoint?).

There are three broad methods of authenticating an individual:

- Something a person knows: for example, a password, a passphrase, response to a secret question, or other piece of knowledge not readily known to others. Although this authentication scheme is the least resource-intensive for the system to implement, it is the most taxing on the user's mental abilities. Knowledge-based authentication schemes do not require specialized hardware, nor do they require a user to retain possession of a token. They shift the burden of proof to the user, who is responsible for memorizing a sequence of characters, numbers, and other tokens, or for responding to a question [4].
- Something a person possesses: this may include tokens such as an identification card or security token. In its simplest form, possession of a token is enough to gain access. In more sophisticated schemes, the token may require additional verification, such as checking if a picture on the security token matches that of the person requesting access.

- An intrinsic characteristic: biometrics. These may be physical traits that we are born with, such as fingerprints or face structure, those that develop over time due to uncontrollable factors, such as patterns in the iris, or learned behaviors (behavioral biometrics). Generally, we seek to use biometrics that exhibit both uniqueness and permanence – those that can uniquely identify an individual and do not change much over time.

Table 1. Methods of authentication

	Something you know	Something you possess	Something you are
Convenience	*(Worse)* Requires memorization	*(Worse)* Must be on person for authentication	*(Better)* Part of the individual
Security	*(Worse)* May be shared, coerced, forgotten, or exposed	*(Worse)* May be shared, coerced, lost, or forged	*(Neutral)* Possible to forge, cannot be lost or forgotten
Suitability for mobile devices	*(Worse)* Long passwords are difficult to type on small devices	*(Worse)* Mobile devices may lack physical hardware needed to validate security tokens	*(Better)* Certain biometrics can be validated with hardware already incorporated into mobile devices
Risk	*(Better)* An exposed password can be invalidated and reset	*(Better)* A lost token can be invalidated and reissued	*(Worse)* We cannot change our biometrics if compromised

Table 1 presents a comparison of these high-level methods of authentication. The three aforementioned methods (something you know, something you possess, something you are) are compared in terms of their convenience, security, suitability for mobile devices, and risk. Each element is rated on a scale of worse, neutral, or better with regards to the specified metric.

- Convenience: convenience is defined as ease of use to the user, not the system. Memorizing passwords and securing tokens rank lower than biometrics, which require no or minimal overhead of the user.
- Security: all three methods have security faults, although biometrics may be more favorable as they cannot as easily be shared.
- Suitability for mobile devices: both passwords and tokens present challenges on mobile devices (such as smartphones). These devices either make it inconvenient to type lengthy passwords repeatedly (where lengthy passwords have been shown to be more secure than shorter ones [36]) or lack hardware needed to validate security tokens. Some biometrics, such as faces and fingerprints, can be validated with hardware now available on mobile devices.

– Risk: we define risk as the risk to the user if their credentials are exposed. Passwords present minimal risk if they are not reused between systems (which, unfortunately, is typically not the case [17]). Lost tokens can be invalidated to prevent their use on systems. In both cases, it is possible for the user to move on with new credentials in the case of a breach. However, the major strength of biometrics – their inseparable association with the individual – makes them a liability if compromised (for example, if someone is able to replicate someone else's fingerprint). In this case, we cannot simply change our fingerprints. The user is dependent on the system implementing a biometric authentication scheme that does not directly store information that can be used to simulate the user's features.

Two-factor authentication is the use of two (or more) authentication modalities, such as requiring a password and a security token, or a fingerprint and a photo ID. While two-factor authentication can improve a system's security, it may impede usability by extending the duration and requirements of the authentication activity. Additionally, two-factor authentication still leaves vulnerabilities exposed [28].

Given the convenience to the user and security of the scheme, the remainder of this work focuses on biometrics as a single factor method of authentication. More specifically, this paper will present behavioral biometrics, which have the additional benefit of being able to be collected without necessarily requiring explicit user action, providing benefits for both security and usability.

4 Behavioral Biometrics

There are two types of biometrics: physical and behavioral. Physical biometrics include fingerprint, facial, and iris recognition. Physical biometrics are derived from unique physical characteristics that are usually determined prior to birth or formed through involuntary muscle movements. Behavioral biometrics are based on our activities and learned reactions, although they are heavily influenced by our physical characteristics. For example, a person's gait depends on their size, weight, and muscle mass.

Behavioral biometrics have a long history of acceptance as a means of verifying an identity. Signatures have been used from ancient to modern times in order to authenticate documents. Today, signatures are one of several options for behavioral biometrics.

Behavioral biometrics are appealing because they can be collected in a less intrusive manner than physical biometrics [13]. Some behavioral biometrics, such as keystroke dynamics (unique typing patterns made by users), can even be collected without any explicit user action. Keystroke dynamics can be recorded in the background as the user types. The wide variety of sensors available on mobile devices (touch, GPS, gyroscope, camera, microphone, among others) provide intriguing options for authentication using behavioral biometrics.

Although promising, behavioral biometrics have several potential pitfalls. From a security perspective, we must be prepared to allow a wide range of acceptable signals. Whereas, for example, a text password must match exactly,

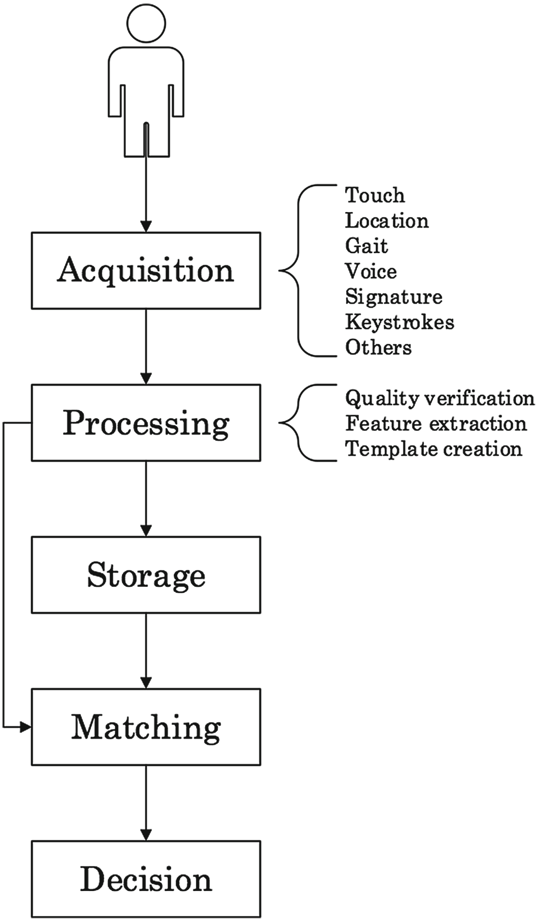

Fig. 1. Overview of a behavioral biometric system

behavioral biometrics can vary depending on a person's mood or stress [18]. Behavioral biometrics are also vulnerable to being imitated by a skilled attacker! [18]. In terms of usability, some behavioral biometrics may not apply to a wide range of users and may impede universal access.

The design of a behavioral biometric system is described in Sect. 4.1. Gait, voice, handwriting, keystroke dynamics, and other behavioral biometrics are presented in Sects. 4.2, 4.3, 4.4, 4.5, and 4.6, respectively.

4.1 Behavioral Biometric System Design

An overview of a behavioral biometric system is shown in Fig. 1. The system has the following stages:

- Acquisition: during the acquisition stage the system will sample signals derived from a user's behaviors. This may require the user to interact with a user interface, such as writing a signature, or it may be done passively, such as recording a voice.

- Processing: the processing stage first ensures the signal recorded is of sufficient quality for further processing. If the signal is inadequate, the system may immediately request a new sample. If the signal is of good quality, features will be extracted. These extracted features are a subset of the original signal – after this point we can discard the original data, if desired. The extracted features are encoded as a template. The format of the template is designed to allow efficient storage, retrieval, and comparison.
- Storage: templates are stored in a database and must be protected against adversaries. Templates may be protected by encryption or by more sophisticated schemes.
- Matching: matching compares the acquired signal to the database in order to compute the similarity between the user currently under consideration and the claimed identity.
- Decision: finally, the system must render a decision – allow or deny. Sometimes, this stage is left up to a human administrator to determine.

4.2 Gait

Gait is the pattern of locomotion individuals make as the move. When people can "recognize a person's footsteps", they are performing a form of gait recognition. Although this is learned behavior, it is impacted by a person's physical characteristics (weight, height, muscle mass, shoes, posture, clothing, motion, etc.) [11,20]. Several methods of gait recognition have been proposed, including using a person's silhouette [33] and readings from an accelerometer [12]. It has been shown that both approaches perform comparably [12]. Many mobile devices are equipped with accelerometers, making gait recognition a potential means of providing access.

4.3 Voice

Voice, or speech recognition is an intriguing behavioral biometric with applications including and beyond authentication. A user's voice can be used to determine their identity using simply a microphone. Performance can be used if the user dictates a specific phrase expected by the system (text dependent), but recognition can also be text-independent [25]. Speech is a natural part of many transactions and is not considered to be as intrusive as providing a fingerprint or even taking a picture. Furthermore, voice provides additional cues about a user's stress level that can be used to improve the performance of the system.

4.4 Handwriting

Handwriting, including signatures, can be used to identify users. This identification can be performed by identifying characteristics such as the number of strokes made, timing, count of pen up and pen down motions, and several proportions and areas formed by the written information [31]. As with several other behavioral biometrics, handwriting recognition can be vulnerable to attack [21]. However, handwriting is remarkably versatile and a natural input method for touch surfaces.

4.5 Keystroke Dynamics

Keystroke dynamics can be used to identify a person based on the timing between subsequent keystrokes. Although originally intended for physical, mechanical keyboards [23], keystroke dynamics have been implemented on mobile devices [16]. Interestingly, keystroke dynamics have also shown promise as a way for determining a user's emotional state (such as nervousness or tiredness) [10].

4.6 Other Behavioral Biometrics

Many other behavioral biometrics are available. Behaviors ranging from game strategy [34] to musical proficiency [9] can be used to authenticate individuals. A detailed survey of behavioral biometrics is available in [35]. While new schemes will continue to be developed, it is important to evaluate them on both their security and usability qualities.

5 Discussion and Conclusion

Many users do not use any or only minimal protection on their mobile devices [15]. Users to not seek to "do security", they aim to complete their intended tasks in the most efficient way possible. Generally, this relegates security to a burdensome task. Behavioral biometrics (and biometrics in general) are an attractive alternative. Behavioral biometrics can provide a degree of authentication for minimal user interaction.

However, we must also consider the implications widespread use of behavioral biometrics would have for universal access. Certain behavioral biometrics may exclude groups of people. For example, gait assumes a person is able to walk. Voice recognition requires a person who can speak. Poor usability of implementations of behavioral biometrics can lead to a high rate of false positive errors (allowing unauthorized users access). By definition, behavioral biometrics reflect the behavior of the user. The system must be able to guide the user's behavior in a consistent manner in order to achieve reliable authentication to as wide a range of users as possible.

Behavioral biometrics provide opportunities for universal access beyond authentication. For example, the ability to know the user's current emotional state can be incorporated into system behavior. Perhaps a user who is upset should have access to only a restricted set of features. Or, a user who is confused could be provided additional assistance.

This work discussed security and authentication considerations of universal access systems and then considered the utility of behavioral biometrics. Although behavioral biometrics provide intriguing opportunities for authentication users, their use must be moderated by security and usability requirements.

References

1. Al-Harby, F., Qahwaji, R., Kamala, M.: Users acceptance of secure biometrics authentication system: reliability and validate of an extended utaut model. In: Zavoral, F., Yaghob, J., Pichappan, P., El-Qawasmeh, E. (eds.) Networked Digital Technologies, pp. 254–258. Springer, Heidelberg (2010)
2. Bahr, G., Mayron, L., Gacey, H.: Cyber risks to secure and private universal access. In: Stephanidis, C. (ed.) Universal Access in Human-Computer Interaction. Design for All and eInclusion, Lecture Notes in Computer Science, vol. 6765, pp. 433–442. Springer, Berlin Heidelberg (2011)
3. Braz, C., Robert, J.: Security and usability: the case of the user authentication methods. In: Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine, pp. 199–203. ACM (2006)
4. Brostoff, S., Sasse, M.A.: Are passfaces more usable than passwords? a field trial investigation. People and Computers, pp. 405–424. Springer, London (2000)
5. Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. In: Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 426, pp. 233–271. The Royal Society (1989)
6. Bursztein, E., Bethard, S.: Decaptcha: breaking 75% of ebay audio captchas. In: Proceedings of the 3rd USENIX conference on Offensive technologies, p. 8. USENIX Association (2009)
7. Cohen, S., Ben-Asher, N., Meyer, J.: Towards information technology security for universal access. In: Stephanidis, C. (ed.) Universal Access in HCI, Part I, HCII 2011. LNCS, vol. 6765, pp. 443–451. Springer, Heidelberg (2011)
8. Cranor, L., Garfinkel, S.: Guest editors' introduction: secure or usable? IEEE Secur. Priv. **2**(5), 16–18 (2004)
9. Dalla Bella, S., Palmer, C.: Personal identifiers in musicians' finger movement dynamics. J. Cog. Neurosci. **18**, G84 (2006)
10. Epp, C., Lippold, M., Mandryk, R.L.: Identifying emotional states using keystroke dynamics. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 715–724. ACM (2011)
11. Gafurov, D.: A survey of biometric gait recognition: approaches, security and challenges. In: Annual Norwegian Computer Science Conference, pp. 19–21. Citeseer (2007)
12. Gafurov, D., Helkala, K., Søndrol, T.: Biometric gait authentication using accelerometer sensor. J. Comput. **1**(7), 51–59 (2006)
13. Gamboa, H., Fred, A.: A behavioral biometric system based on human-computer interaction. In: Defense and Security, pp. 381–392. International Society for Optics and Photonics (2004)
14. Greene, S.: Security Policies and Procedures: Principles and Practices (Prentice Hall Security Series). Prentice-Hall Inc, Upper Saddle River (2005)
15. Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A., Smith, M.: Itsa hard lock life: a field study of smartphone (un) locking behavior and risk perception. In: Symposium on Usable Privacy and Security (SOUPS) (2014)
16. Hwang, S., Cho, S., Park, S.: Keystroke dynamics-based authentication for mobile devices. Comput. Secur. **28**(1), 85–93 (2009)
17. Ives, B., Walsh, K.R., Schneider, H.: The domino effect of password reuse. Commun. ACM **47**(4), 75–78 (2004)
18. Jain, A., Ross, A., Nandakumar, K.: Introduction to Biometrics. Springer, US (2011)

19. Kumar, N.: Password in practice: a usability study. J. Global Res. Comput. Sci. **2**(5), 107–112 (2011)
20. Lee, L., Grimson, W.E.L.: Gait analysis for recognition and classification. In: Proceedings Fifth IEEE International Conference on Automatic Face and Gesture Recognition, pp. 148–155. IEEE (2002)
21. Lopresti, D.P., Raim, J.D.: The effectiveness of generative attacks on an online handwriting biometric. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 1090–1099. Springer, Heidelberg (2005)
22. Mayron, L.M., Hausawi, Y., Bahr, G.S.: Secure, usable biometric authentication systems. In: Stephanidis, C., Antona, M. (eds.) UAHCI 2013, Part I. LNCS, vol. 8009, pp. 195–204. Springer, Heidelberg (2013)
23. Monrose, F., Rubin, A.D.: Keystroke dynamics as a biometric for authentication. Future Gener. Comput. Syst. **16**(4), 351–359 (2000)
24. Pfleeger, C., Pfleeger, S.: Security in Computing. Prentice Hall PTR, Englewood Cliffs (2006)
25. Reynolds, D.A.: An overview of automatic speaker recognition. In: Proceedings of the International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. S.4072–S.4075 (2002)
26. Sasse, M.: Computer security: anatomy of a usability disaster, and a plan for recovery. In: Proceedings of CHI 2003 Workshop on HCI and Security Systems. Citeseer (2003)
27. Sasse, M., Brostoff, S., Weirich, D.: Transforming the weakest linka human/computer interaction approach to usable and effective security. BT Technol. J. **19**(3), 122–131 (2001)
28. Schneier, B.: Two-factor authentication: too little, too late. Commun. ACM **48**(4), 136 (2005)
29. Stephanidis, C.: The Universal Access Handbook. CRC Press, Boca Raton (2009)
30. Toledano, D., Fernández Pozo, R., Hernández Trapote, Á., Hernández Gómez, L.: Usability evaluation of multi-modal biometric verification systems. Interact. Comput. **18**(5), 1101–1122 (2006)
31. Vielhauer, C., Steinmetz, R., Mayerhofer, A.: Biometric hash based on statistical features of online signatures. In: Proceedings of 16th International Conference on Pattern Recognition, vol. 1, pp. 123–126. IEEE (2002)
32. Von Ahn, L., Maurer, B., McMillen, C., Abraham, D., Blum, M.: reCAPTCHA: Human-based character recognition via web security measures. Science **321**(5895), 1465–1468 (2008)
33. Wang, L., Tan, T., Ning, H., Hu, W.: Silhouette analysis-based gait recognition for human identification. IEEE Trans. Pattern Analy. Mach. Intell. **25**(12), 1505–1518 (2003)
34. Yampolskiy, R.V.: Mimicry attack on strategy-based behavioral biometric. In: Fifth International Conference on Information Technology: New Generations, ITNG 2008, pp. 916–921. IEEE (2008)
35. Yampolskiy, R.V., Govindaraju, V.: Behavioural biometrics: a survey and classification. Int. J. Biom. **1**(1), 81–113 (2008)
36. Yan, J., et al.: Password memorability and security: empirical results. IEEE Secur. Priv. **5**, 25–31 (2004)