Secure, Usable Biometric Authentication Systems

Liam M. Mayron, Yasser Hausawi, and Gisela Susanne Bahr

Florida Institute of Technology, Melbourne, FL 32901, USA
{lmayron,gbahr}@fit.edu, yhausawi@my.fit.edu

Abstract. Biometrics are physiological features that allow individuals to be identified. Popular biometrics include fingerprints, faces, and irises. A common use of biometric systems is to authenticate users desiring access to a system or resource. Universal Access can be promoted with biometrics. Biometrics provide a secure way to access information technology, although the use of biometrics presents challenges and opportunities unique to other authentication methods (such as passwords and tokens). Biometric systems are also vulnerable to poor usability. Such systems must be engineered with wide user accessibility and acceptability in mind, but also need to provide robust security. This paper considers the application of biometrics in Universal Access systems with regards to usability and security.

Keywords: universal access, biometrics, security, usability.

1 Introduction

Universal Access (UA) seeks to provide the utility of modern information technology to as broad a range of individuals as possible [1]. Security is essential to the functionality of this technology, although it is seldom the subject of universal access research [2]. As real-world adoption of UA increases, so too will the severity of related security and privacy issues.

There are several ways to implement security in conjunction with UA. This work focuses on biometric authentication technologies. Biometrics are unique physiological features that can be used to authenticate a person's identity. There are a variety of biometrics, including fingerprint, face, iris, gait, palm print, and voice. Fingerprints are the most commonly used biometrics due to their widespread acceptance and usability [3, 4]. Face recognition has been favored in research environments due to the availability of face databases for development, although iris recognition may ultimately provided superior accuracy [5]. The selection of a biometric trait for a particular system depends on many environmental and situational factors.

Biometrics are a natural choice for implementing authentication in UA systems [6]. Biometrics are more usable than memorization- and physical token-based methods of authentication, although the usage of biometrics can introduce

C. Stephanidis and M. Antona (Eds.): UAHCI/HCII 2013, Part I, LNCS 8009, pp. 195–204, 2013.

risks as severe as permanently compromising an individual's security [6]. The potential to integrate security and usability effectively is greater with biometrics than with other authentication methods [7–11]. Traditional methods of authentication, including passwords, identification cards, and tokens, have not yet been able to bridge the gap between security and usability in UA systems [9].

If properly implemented, biometrics can reconcile security and usability disadvantages of authenticating users without the need for memorization or tokens. This work investigates both the usability and security of biometric systems within the context of UA.

The remainder of this paper is organized as follows. Security is discussed in Section 2. Section 3 presents biometric systems in the context of authentication. Usability topics are treated in Section 4, while usable security is considered in Section 5. The application of usable security to biometric authentication is shown in Section 6. Conclusions appear in Section 7.

2 Security

Security is important in UA systems. In many scenarios, UA provides access to sensitive, personal information – in these cases, privacy must be maintained. In other cases, UA systems can be integrated with broader computational infrastructure. Here, UA should not introduce additional security vulnerabilities. Of particular concern to UA systems are consumer data, health data, demographics, and location privacy [2]. For example, use of a UA system may unintentionally expose a user's geographic location or demographic information.

Cybersecurity can be summarized as a set of methods and techniques that guard against adversaries. These methods are essential to modern computation. Contemporary information technology environments are characterized by increasingly common persistent connections to the outside world (or even just internal networks) and massive collections of data. Adversaries constantly seek to obtain or compromise this data through these external access points.

At a high-level, there are three key requirements for securing a system. The system must be able to provide confidentiality, integrity, and availability [12, 13]. These security requirements may cause tension with both UA and usability objectives (discussed later in the paper). As UA seeks to provide access to information in a broad and accessible manner, appropriate safeguards must be put in place. These safeguards must ensure that data privacy is ensured (confidentiality), that data cannot be modified without consent (integrity), and that the data is present and accessible when needed (availability).

As adoption of UA systems increases, so too will threats to security. Security must be considered alongside usability in the design of UA systems. The following section discusses biometrics and their role in securing systems. Subsequently, usability is considered.

3 Biometrics

UA aims to provide the benefits of information technology to all individuals, but this access must be provided in a secure manner. Information should only be provided to those with the proper credentials and permissions. Biometric are a potential solution to implementing authentication within the context of UA.

Central to the secure access of UA systems is authentication. Individuals may authenticate with a system by providing one or (preferably) more of the following:

- Knowledge: for example, a password or response to a question. Such knowledge should be unique to the individual or group needing access to the resource. Security depends on the knowledge remaining secret
- Proof of possession: this may be an identification card or other token. Possession of the token is used to determine if a claimed identity is genuine (e.g. the token may contain a picture of a person or be used in conjunction with other methods of authentication)
- Intrinsic characteristics: biometrics – for most individuals, these are physiological characteristics we are born with – they cannot be lost of forgotten

There are benefits and drawbacks to each of the three methods of authentication. Knowledge-based methods are straightforward to implement, but result in increased cognitive load on the user due to having to remember their credentials [14]. Compounding this, knowledge may be forgotten or shared with an adversary. More complex password requirements can provide better security, but at the expense of usability because longer passwords burden users with the more complex password creation, memorization, and recall. Simple passwords are more usable but less secure (shorter passwords are easier to attack). Token-based methods require possession of a physical item to gain access, which is not always practical. The physical token may be lost, forged, or stolen. Biometrics are always on-person (in the cases where the person is able to provide the biometric). They cannot be forgotten. Biometrics are more tightly-connected to an individual's identity than passwords or tokens. The main weakness is that in the event biometrics information is forged or stolen, an individual may not be able to access any systems – the information cannot be changed.

Biometric authentication systems produce an authentication decision based on a comparison to user-provided input and a database of previously-sampled records. The method of producing an authentication decision may be supplemented with a human administrator and an exception mechanism for cases where the biometric data cannot be presented or recorded. The components of a biometric system include humans (both users and administrators), software, and hardware. A general overview of a biometric system is shown in Figure 1.

The *user* is the subject with regards to which the system must make a decision. The user can interact with the system directly and explicitly (for example, presenting their fingers to a scanner), or indirectly (such as when a photograph is used for facial recognition).

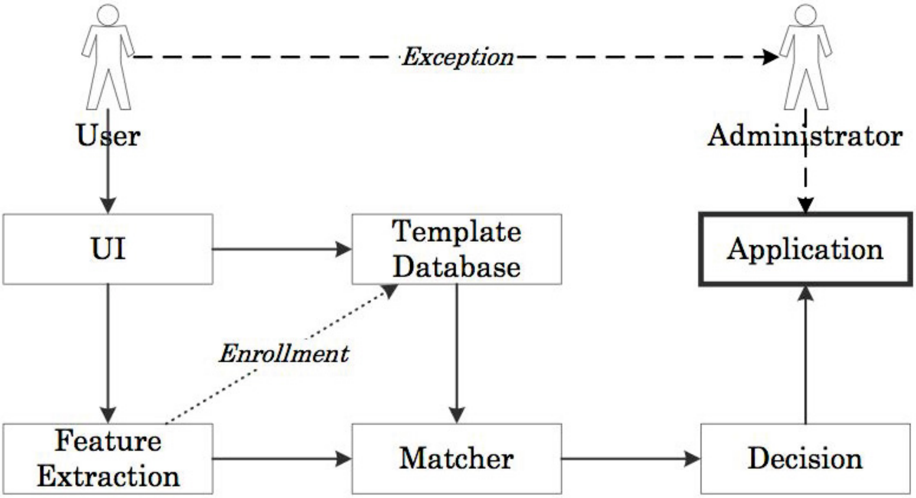


Fig. 1. Overview of a biometric system

The *administrator* handles system *exceptions*. Biometric systems must often provide an alternate method of authentication (such as a photo identification card) in the event the primary method of verification does not work. This may happen coincidentally (perhaps due to poor sensors or directions), due to a missing trait in the user, or explicitly – as part of a deliberate attack. The administrator must verify the user's credentials using the alternate means and make the authorization decision manually.

The *user interface* may be hardware, software, or a combination of both. It can be visible or invisible to the user. The role of the user interface is to collect the required biometric information in a reliable manner. A poor user interface risks false negatives and frustrating legitimate users. A good user interface provides a better experience and potentially better security.

The *feature extraction* module translates the successfully sampled data into a more compact alternative representation – a *template*. The purpose of the templates is to reduce storage requirements (for example, instead of storing am image, a much smaller feature vector may suffice) and to reduce the time needed to compare biometric samples time. Generally, most of the original sample is discarded after feature extraction and only the template is maintained.

The *template database* stores the extracted data. An entry in the template database is created the first time the user accesses the system. Subsequent authorization attempts are verified against the entries in the template database.

The *matcher* compares the template generated from the current access attempt to the information stored in the template database. Generally, a threshold is used in order to render a decision. Matching can be challenging as it is unlikely (and suspicious) to have a perfect match – a certain degree of dissimilarity must be permitted. Matching results in a *decision* (allow or deny access), which is forwarded to the *application*.

Authentication begins by acquiring biometrics traits from the user. These traits are acquired using a sensor tailored for that particular modality. The sampled data is then processed to isolate the desired trait and reduce or assess the amount of noise present. The processed traits are transformed into templates and stored. Subsequently, stored templates can be compared to new samples in order to allow or reject a person desiring access [5].

There are many different biometrics, and many ways each of the processing steps can be performed. As a result, each sub-process may have its own usability and security concerns. However, these sub-processes have not yet been investigated in terms of usable security [15].

4 Usability

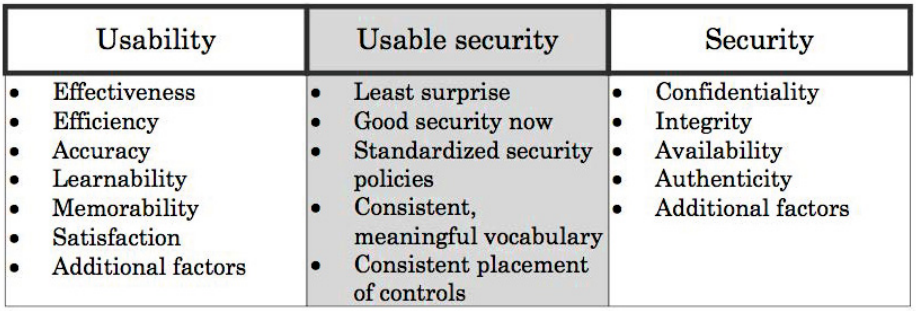
Usability is defined as the range that legitimate users can operate a product to preform particular tasks in specified methodology with an accepted level of satisfaction, and in an effective and efficient way [16]. Usability is essential to UA ("universal usability") [17]. Information and services should not only be made available to all, but be made usable for everyone as well.

Usability is evaluated by testing one or more constituent factors (including product effectiveness, efficiency, learnability, memorability, accuracy, and user satisfaction). Effectiveness is described as the user's ability to successfully achieve the goal of operating such a product. Efficiency is defined as user's ability to successfully perform a particular task and complete it within an acceptable timeframe. Satisfaction is the user'a degree of happiness of operating a product [18]. Learnability is the user's ability to learn how to operate a product. Memorability is user's ability to remember how a product is operated and also remember the required information to operate such a product. Finally, accuracy is defined as user's ability to operate a product and obtain accurate results. There are many other human, environmental, hardware, and software characteristics that are impacted by usability. The factors that are important to creating usable systems are also key to UA.

5 Usable Security

In certain situations the objectives of usability and security can compete against each other. In others, security is implemented, but not in a fashion that is intuitive to the user. Security in software is usable if users are made aware of the security tasks to perform, how to perform those tasks, and how to prevent dangerous errors, all while maintaining comfort with the user interface [19]. Usable security mechanisms are a set of techniques and methods for security that are usable for genuine users, but not for adversaries [8].

Figure 2 shows the intersection between usability and security from a user-centered design perspective. Each of the usable security principles [20] shown in Figure 2 is a result of a combination of usability and security considerations. The principle of *least surprise* maintains that security mechanisms and users should



Usability	Usable security	Security
• Effectiveness • Efficiency • Accuracy • Learnability • Memorability • Satisfaction • Additional factors	• Least surprise • Good security now • Standardized security policies • Consistent, meaningful vocabulary • Consistent placement of controls	• Confidentiality • Integrity • Availability • Authenticity • Additional factors

Fig. 2. Usable security lies at the intersection of usability and security [20]

have mutual cooperation, understanding, and expectations – users should be aware of the tasks that must be performed [20]. The *good security now* principle prescribes that available security technology is better than none at all [20]. *Standardized security policies* are preferred to frequently customized ones as they are easier for users to understand [20]. Similarly, a *consistent, meaningful vocabulary* should be applied and appropriate terms used to convey intended ideas and concepts [20]. *Consistent placement of controls* improves the mental stability and perception of users [20].

Security and usability in UA systems must be considered together, through a usable security approach that extends from the initial concept through development and then maintenance. Application of the usable security requirements and principles can guide development towards more effective implementations of both usability and security.

6 Usable Security for Biometric Authentication

Biometrics authentication systems have promise as gateways to UA. This potential must be tempered by both usability and security considerations. A substantial amount of research has investigated the use of biometrics for authentication in order to address the usability-security conflict. Sasse et al. anticipated that biometrics in combination with security systems may be suitable for user, task, and context configuration [11]. Sasse also claimed that biometrics can reduce both the physical and mental load placed on users despite privacy-related risks [10]. Cranor et al. stated that biometric systems should be used in lieu of passwords for authentication [8]. Kumar also recommended alternative authentication schemes including biometrics in place of alphanumeric passwords due to the better usability of biometrics [9]. Braz and Robert suggested that biometric systems in combination with other methods of authentication (e.g. passwords and identification cards) would produce robust, usable, and secure authentication systems. [7].

Usability considerations affect nearly all aspects of biometric systems, from the early design to operations. The selection of the biometric itself is critical. A comparison of the usability of three types of biometrics (fingerprint, signature, and voice) was undertaken in [4], where it was concluded that fingerprints are the most usable among the evaluated traits. However, certain biometrics are not available in all situations. Fingerprints may not be the optimal choice in a dirty environment or cold weather where gloves are worn. Face recognition may be more user-friendly as it can be done from a distance without requiring physical contact.

A cross-cultural survey regarding user acceptance of biometrics in the United Kingdom, India, and South Africa found that culture has a direct impact on user acceptance of biometrics [21]. Al-Harby et al. studied the acceptance of fingerprint biometrics specifically in Saudi Arabia [3].

Errors in biometric systems can be due to hardware, software, or users. Hardware (specifically, sensors) may not be sensitive or reliable enough to sample the desired information (potentially resulting in a failure-to-enroll or failure-to-acquire error). Software algorithms can produce imprecise and inaccurate results resulting in false positives and false negatives. Users can use a system improperly or ineffectively.

In certain cases, sensitivity to errors is a design decision. An implementation may require more restrictive conditions to allowing a user into the system, resulting in an increased number of false negatives (legitimate users who are incorrectly rejected). False negatives reflect poorly on the usability of a system but may be necessary depending on the security context. In contract, a design may deliberately lower the threshold to acceptance, resulting in more false positives (users who are mistakenly accepted).

The design of biometric systems, particularly usable, secure systems for UA, must consider the nature of application. Decisions here can have a significant impact on the design and performance of the implementation. These considerations include [5]:

- User cooperation: will users willingly use the system? A biometric that requires physical contact may not be appropriate if user participation cannot be assured.
- User habituation: a system that will be used only once or seldom may have a different set of usability requirements from a system that is used on a regular basis. This consideration can impact the instructions that are delivered to users, the pace at which the user interacts with the system, the tolerance for errors, and other elements of the user experience. Experienced users may be inconvenienced by steps that are necessary for new users.
- Attendance: the presence of a human operator will alter the usage of a biometric authentication system. A human in attendance can help ensure proper usage of an authentication mechanism. An unattended system must be able to anticipate a wider range of contingencies.
- Control: certain biometrics, such as face recognition, are sensitive to environmental factors, whereas others, like fingerprint sensors, can be placed in a fixed position that is not sensitive to light, wind, and other factors. User

participation can help with minimizing the impact of uncontrolled environmental factors.

The impact of these factors on two different biometrics – fingerprint and face recognition is considered in the following subsections.

6.1 Fingerprints

Fingerprints are patterns of ridges and valleys at the extremes of our digits that help us grab and feel items and surfaces. They consist of several patterns – arches, wholes, and loops. There is a large body of cases where fingerprints have been used in forensic investigations to determine an identity. The patterns on fingerprints are produces by the random stresses that occur during gestation [5].

Fingerprints are recognized by analyzing key points known as minutiae. Minutiae occur at locations where ridges terminate or split – ridge endings and bifurcations. The relative locations and orientations of minutiae can be represented as a compact template and efficiently compared to other templates.

The process of fingerprint recognition begins with sampling the finger. A variety of technologies (e.g. thermal, capacitance, reflectivity, and others) can be used to map the ridges and valleys. This map – an image – is processed in order to determine the location of minutiae. The accurate accounting of minutiae locations and orientations is key to the performance of fingerprint recognition systems.

Poor usability can decrease the performance of fingerprint recognition systems and frustrate users. For example, a failure-to-acquire error can be caused by users pressing their finger against the sensor improperly. The temperature of the environment can also impact the ability to sense fingerprints. A usable system that correctly guides users and system operators to presenting fingerprint and credential information in an effective way can reduce technical errors and improve security. Consequently, when usability-related technical errors are reduced and security is improved, fingerprint recognition systems can be more effectively, efficiently, and satisfactorily used in UA.

6.2 Face Recognition

Face recognition is a popular method of biometric authentication. It can be accomplished using cameras that are increasingly available and affordable. For example, a smartphone camera could potentially be used to authenticate a user without the need for any extra hardware. In contrast to fingerprint recognition, face recognition does not require physical contact.

Global characteristics, face geometry, the structure of facial components, and the presence of landmark points can all be used to distinguish faces, although there are a number of challenges. The uniqueness of faces can be difficult to determine without sophisticated (high resolution) sensors, and there is a large degree of similarity between relatives (and certainly twins). Compounding this, faces change over time. Over long periods of time, people grow and age. Even in the short term, facial hair or fashion (e.g. hats, sunglasses) may change. All of these factors present challenges to facial recognition.

Facial recognition begins by taking an image. This image is processed to detect the presence of one (or more) faces within the image. Then, the detected faces are segmented. Templates can be generated using a variety of algorithms. An important component of face recognition systems is liveness detection – otherwise, a system may be fooled by a photograph.

The performance of face recognition systems is greatly affected by the behavior of users. A face that is recognizable indoors during the day may not be outside that same evening. In certain cases, the timing of the system's use is under user control. Similarly, a user may need to remove their glasses to improve the system's accuracy. Factors that are within a user's control can be kept consistent in order to improve performance and security.

7 Conclusion

Universal Access is an important area of research and development that aims to provide access to information technology to everyone. Both security and usability are essential to UA, and each has their own technical challenges. Resolutions to these challenges can sometimes be in conflict. Biometrics can be used to provide security to UA systems in a potentially more usable and effective manner. System designers must be aware of the specific impediments to the effective implementation of biometric systems. Poor usability of biometrics can adversely impact the security of a system. A comprehensive UA system design must consider security and usability together.

References

1. Stephanidis, C.: The Universal Access Handbook. CRC (2009)
2. Bahr, G.S., Mayron, L.M., Gacey, H.J.: Cyber risks to secure and private universal access. In: Stephanidis, C. (ed.) Universal Access in HCI, Part I, HCII 2011. LNCS, vol. 6765, pp. 433–442. Springer, Heidelberg (2011)
3. Al-Harby, F., Qahwaji, R., Kamala, M.: Users acceptance of secure biometrics authentication system: Reliability and validate of an extended utaut model. Networked Digital Technologies, 254–258 (2010)
4. Toledano, D., Fernández Pozo, R., Hernández Trapote, Á., Hernández Gómez, L.: Usability evaluation of multi-modal biometric verification systems. Interacting with Computers 18(5), 1101–1122 (2006)
5. Jain, A., Ross, A., Nandakumar, K.: Introduction to biometrics. Springer (2011)
6. 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)
7. Braz, C., Robert, J.: Security and usability: the case of the user authentication methods. In: Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine, pp. 199–203. ACM (2006)
8. Cranor, L., Garfinkel, S.: Guest editors' introduction: Secure or usable? IEEE Security & Privacy 2(5), 16–18 (2004)

9. Kumar, N.: Password in practice: a usability study. Journal of Global Research in Computer Science 2(5), 107–112 (2011)
10. 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)
11. Sasse, M., Brostoff, S., Weirich, D.: Transforming the weakest linka human/computer interaction approach to usable and effective security. BT Technology Journal 19(3), 122–131 (2001)
12. Greene, S.: Security Policies and Procedures: Principles and Practices. Prentice Hall Security Series. Prentice-Hall, Inc. (2005)
13. Pfleeger, C., Pfleeger, S.: Security in computing. Prentice Hall PTR (2006)
14. Brostoff, S., Sasse, M.A.: Are passfaces more usable than passwords? a field trial investigation. People and Computers, 405–424 (2000)
15. Patrick, A.S.: Usability and acceptability of biometric security systems. In: Juels, A. (ed.) FC 2004. LNCS, vol. 3110, pp. 105–105. Springer, Heidelberg (2004)
16. International Organization for Standardization: 9241-11. Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)–Part II Guidance on Usability (1998)
17. Shneiderman, B.: Universal usability. Communications of the ACM 43(5), 84–91 (2000)
18. Kainda, R., Flechais, I., Roscoe, A.: Security and usability: Analysis and evaluation. In: ARES 2010 International Conference on Availability, Reliability, and Security, pp. 275–282. IEEE (2010)
19. Whitten, A., Tygar, J.: Why johnny cant encrypt: A usability evaluation of pgp 5.0. In: Proceedings of the 8th USENIX Security Symposium, vol. 99. McGraw-Hill (1999)
20. Garfinkel, S.: Design principles and patterns for computer systems that are simultaneously secure and usable. PhD thesis, Massachusetts Institute of Technology (2005)
21. Riley, C., Buckner, K., Johnson, G., Benyon, D.: Culture & biometrics: regional differences in the perception of biometric authentication technologies. AI & society 24(3), 295–306 (2009)