SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 7, NO. 4
ISSN: 2054 -7420

Role of Usability on using Biometrics for Cybersecurity

Yasser M. Hausawi,
Department of Information Technology, Institute of Public Administration, Jeddah, SA
Hawsawiy@ipa.edu.sa

ABSTRACT

Biometrics are traits that allow individuals to be identified. Popular biometrics include fingerprints, faces, and irides. A common use of biometric systems is for authentication of users desiring access to a system or resource. However, 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 must still provide robust security as well. As lack of usability causes systems' failures, and enhancing systems' usability reduces such failures. This article first presents an overview of biometric systems employed today, including their usage and security merits. We then consider the specific role usability plays on both the development and long-term utility of biometric systems used for Cybersecurity.

Keywords: Biometrics; Cybersecurity; Usability; Authentication.

1 Introduction

Biometrics technology is one of the current wide spread technology that is used in many ways. Biometrics can be used to identify and recognize individuals, investigate criminal incidents, prove civil rights, and many others. One focal biometric area is authentication [1]. Biometric systems are well known by their accurate and sophisticated way of recognizing and identifying individuals for authentication purposes. As a result of the previous features, biometrics researchers have come up with many approaches and algorithms that are used to facilitate using such technology and make it usable in our daily life activities. There are many available biometric traits can be used, such as fingerprints, face, iris, gait, palm prints, voice, and many more. Among all, fingerprint is the most commonly used because of its universal acceptance by users in terms of real life usability [2-3], but face is preferred in laboratories because of the availability of face databases and the need for training images, where iris is believed to be the best in terms of accuracy [4]. However, choosing an appropriate biometric trait depends on many environmental and situational factors. Indeed, one primary reason for considering biometrics as authentication technology in security mechanisms is that such technology ties usability and security together to provide usable security for computing systems in a better way than other authentication methods [4-8, 13]. As all traditional authentication methodology like passwords, identification cards, and tokens could not sufficiently close the gap between usability and security [7]. The traditional authentication methodology relies on one of the two approaches, knowledge-based approach (like passwords), or possession-based

DOI: 10.14738/tnc.74.7244
Publication Date: 28th October 2019
URL: http://dx.doi.org/10.14738/tnc.74.7244

approach (like tokens). Both of the approaches share some disadvantages that negatively impact usability, security, or both simultaneously. For example, a more complex password mechanism helps in better security, but its unusable when users create, memorize, and use such complex passwords. In contrast, an easy password mechanism helps in better usability, but it becomes very difficult to maintain security. Not like the previous authentication methods, biometrics authentication relies on existence-based (who you are) approach. This approach, if properly engineered and applied, can address the disadvantages of the two traditional approaches. As properly developed biometrics authentication methodology can improve both usability and security together to provide usable security for computing systems. However, it brings privacy issues out of the scope of this paper.

Therefore, this article focuses not only on biometrics security or biometrics usability, rather, it focuses on analyzing both usability and security together in order to provide usable security guidelines for biometric authentication building blocks and design cycle. Next section is a motivation to secure and usable biometrics authentication. Section 3 displays related work done on biometrics from usability - security viewpoint. In addition, this section presents an overview of security, usability, and biometric systems employed today, including their usage. Section 4 discusses the basic building block of biometric systems from usability security viewpoint. Section 5 provides case studies and usable security guidelines for biometric authentication, and finally, section 6 is conclusion and future work.

2 Motivation

There are many researchers have considered and claimed that using biometrics in security systems for authentication purposes would solve the intricate nature of usability security conflict. M. A. Sasse et. al. anticipated that biometrics, when used in security systems, may be suitable for user / task / context configuration in some security cases [8]. In another research work, Sasse also claimed that biometrics can reduce both physical and mental load on users despite of the privacy related risk [13]. Lorrie Cranor at. el. Stated that biometrics systems are strongly suggested for security systems rather than traditional password systems [6]. Likewise, Naveen Kumar recommended alternative authentication schemes such as fingerprint authentication (biometrics) in place of alphanumeric passwords, because biometrics can help in better usable security systems [7]. Same way, Christina Braz and Jean-Marc Robert suggested that biometrics systems, when used along with another authentication system (passwords, ID's), would come up with such robust usable and secure authentication systems [5]. Next section gives some background about usability and security of biometrics.

3 Background

As a response to the above promising and motivating claims of the previous section, there have been a few studies conducted in many ways (experimental and theoretical) to evaluate biometrics systems in terms of usability [14]. The following lists the related work of interacting security and usability on biometrics.

3.1 Related Work

Biometric traits issues: Toledano et. al. conducted a usability evaluation study on biometrics systems. They evaluated the usability of three different biometric traits, that are: fingerprint, signature, and voice. According to Toledano and his coauthors, fingerprint is proven to be the best among all of the evaluated traits [2].

Cultural issues: Chris Riley et. al. did a cross-cultural survey about acceptance of using biometrics authentication technologies in three cultural different countries (The UK, India and South Africa). They found out that culture has direct impact on users' level of acceptance of using biometrics technologies, as the result showed that the degree of cultural concern about privacy and the degree of trust affect users'' acceptance of using biometrics technology. This study has brought the rule of cultures in usability of using biometrics as security authentication technologies [9]. Fahad Al-Harby et. al. wrote a paper on users' acceptance of secure biometrics authentication. The authors based their study on one biometric trait (fingerprint) to find out the factors that affect users' acceptance to such technology in Saudi Arabia [3].

Performance issues: Belen Fernandez Saavedra et. al. come up with an evaluation methodology to analyze and evaluate usability factors that affect biometric performance. The methodology was checked for one trait (fingerprint), and proved that it is a useful biometrics performance usability factors evaluation methodology [10]. Eric Kukula et. al. provided an evaluation method for biometric performance usability measurements effects. The idea of the methodology focuses on generating additional more focused measures from the traditional system-level evaluation metrics (The failure-to-acquire(FTA),the failure-to-enroll (FTA), the false-accept (FAR), and the false-reject(FAT)), as The authors claimed that using the above metrics for evaluation is not enough to evaluate the usability of biometric performance, and they proved that the new generated metrics improved the biometric performance evaluation because the new metrics analyze the interaction between humans and biometric sensors in a more accurate way[11].

3.2 Biometrics

Biometric authentication process is divided into many sub-processes starting by biometric traits acquisition, and ending by identity authentication as shown in Figure 1. Throughout this multi-part process, a particular biometric trait is acquired using acquisition devices (sensors or readers) such as fingerprint sensors for fingerprints, cameras and videos for faces, near-infrared sensors for iris, and microphones for voice. Using the sensors and readers, a biometric trait is detected and isolated from the rest of the surroundings using specific algorithms such as Viola-Jones for face, Integro-Differential Operator and Geodesic Active Contours for iris, biometrics features are extracted using method such as Poincare index for fingerprints, and algorithms such as Principal Component Analysis (PCA), Independent Component Analysis (ICA), Linear Discriminant Analysis (LDA), Active appearance Model (AAM), Scale Invariant Feature Transformation (SIFT), and Local Binary Patterns (LBP). After that, the extracted biometrics features are stored in a database as templates along with their identities during the enrollment and then matched against other features to provide enough matching information for the decision makers. There are many methods can be used to match biometric features, for example, Manhattan Distance (L1), Euclidean Distance (L2), and Cosine Similarity [4].

Based on the above description of the biometrics authentication processes, almost each sub-process has many ways (algorithms, techniques, or methods) to be performed. Therefore, there are many evaluation studies of each sub-process's ways have been done to find out the most appropriate way used in each sub-process in terms of performance. To that end, there are many evaluation curves used to compare the performance between the different ways of each sub-process. One evaluation curve is called Receiver Operating Characteristics (ROC). Another one is called Precision Recall (PR). Others are Detection Error Trade-off (DET), and Cumulative Match Characteristics (CMC). However, those sub-processes have not been investigated enough in terms of usable security [14]. Moreover, no guidelines are available to ensure the usability and security of each sub-process of biometrics authentication process.

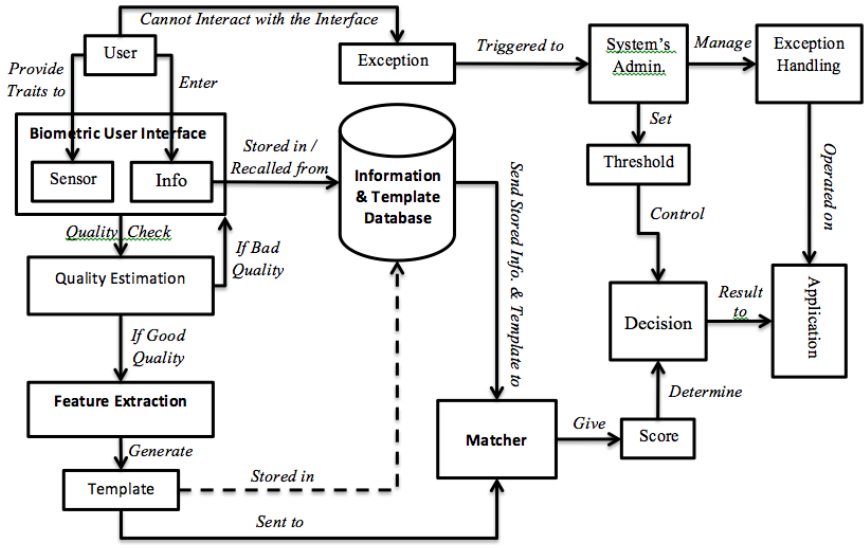

Figure 1: Biometrics Authentication Building Blocks

3.3 Security

Security is also one of the main quality factors. There are two types of security. The first type is the physical security, while the second is the digital or computer security. The scope of this article only covers the digital part. There are many definitions available for computer security, but all of those definitions can be summarized in one unified definition that is: security is a set of methods and techniques that work together to protect weaknesses from the adversaries, and make the meaning of information unclear to unauthorized users. This can be achievable via applying three security sub-factors on computer systems that are: confidentiality, integrity, and availability [1]. In addition, there are other sub-factors added to the security sub-factors, such as authenticity. Confidentiality is described as the ability of security mechanism to protect the information and / or resources from being accessed by unauthorized users. Integrity is a core security sub-factor and defined as the ability to keep the information and / or resources accurate and protect them from being used or altered in an unauthorized way. Availability is security mechanism's ability to ensure information and / or resources existence to be accessed by genuine users at any promised time.

Based on the above illustration of security, any biometrics authentication system must ensure such quality factor. As biometrics authentication systems are claimed by many studies and researchers to provide a better security than the traditional authentication systems such as tokens and alphanumeric passwords [4].

3.4 Usability

Usability is considered as one of the main quality factors that itself has many sub-factors. According to the International Standard Organization (ISO), usability is 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 [12]. Moreover, other researchers included some other usability sub-factors, such as learnability, memorability, and accuracy to the pervious list [12].

Usability is evaluated via testing some or perhaps all of the sub-factors mentioned above (product effectiveness and efficiency, and user satisfaction, learnability, memorability, and accuracy). Effectiveness is described as 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 user degree of happiness of operating a product [16]. Learnability is 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. And finally, accuracy is defined as user's ability to operate a product and get accurate results. There are many other human, environmental, hardware, and software characteristics and factors impacted by usability. The characteristics and factors are listed on Table 1 in section 4.

Based on the above illustration of usability, any biometrics authentication system must achieve such quality factor. As mentioned on the introduction of this article, biometrics authentication systems are claimed by many studies and researchers to provide a better degree of usability than the traditional authentication systems such as alphanumeric passwords.

4 Usable security

Looking at biometrics authentication process from usability and security viewpoint, each of the blocks that perform a particular sub-process deals with either usability or security in a way or another. In addition, some blocks deal with both of usability and security simultaneously, being as an appropriate potential area for the intricate conflict between usability and security. Figure 2 shows the areas that deal with usability in light blue color, and the areas that deal with security in light red color. The interaction between the two colors represent the areas that deal with the usability security conflict.

The most obvious usability area is the interaction between the users and the biometric systems [11]. That area has to be usable enough to biometrics authentication systems' users in order for them to interact properly and easily with the system. As there are many factors can affect usability in the area, such as human factors [8, 3], environmental factors [4], hardware (sensors) quality factors [14], and software quality factors. All of the previously mentioned factors are impacted by usability in either positive or negative ways [10].

Another usability area is when the system administrator excepts some users from interacting with the biometrics authentication interface due to inability to interact with the interface. The human factors play a major role in usability, because both users and systems' administrators are human beings. Last area of usability is the way that the systems' application reacts towards the users based on the matching resulted decision.

There are many important blocks that need to be highly secured in order to have reliable biometrics authentication as highlighted in light red color on Figure 2. One area is the area of interaction between users and the biometrics systems, as such area can affect security because most of the threads start by using users' biometrics traits to attack the biometrics authentication in many ways. For instance, impersonation, obfuscation, and spoofing are some kinds of possible attacks on that area [4].

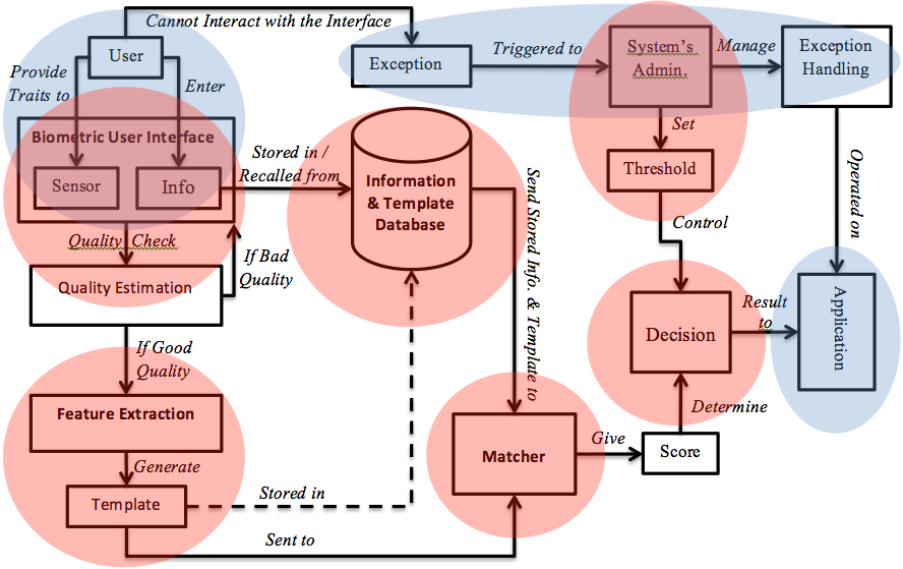

Figure 2: Roles of Usability and Security for Biometric Systems Building Blocks

Other blocks such as quality estimation, feature extraction, matching, and decision; all can be targeted to negatively impact security through Trojan horse attacks on the software performing quality, extraction, matching, and decision tasks. Systems' administrators set thresholds that controls matching decision, man-in-the-middle and hill-climbing are both kinds of attacks can be used to impact biometrics authentication systems' security through tampering matching decision threshold. Among all blocks mentioned above, information and template databases area seems to be the most important in terms of security despite the fact that it has no direct interaction with the normal users, but because all of the biometrics templates are stored there [4]. Template databases not only impacts security, but it impacts privacy as well.

From the above biometrics authentication building blocks analysis of usability from one side, and security from the other, figure 2 shows some important areas where usability and security are overlapped (intersect). Such areas represent the core of the conflict between usability and security, and the only solution to address such conflict is via achieving usable security mechanisms. Whitten and Tygar in [17] defined the term 'usable security' as "Security software is usable if the people who are expected to use it: (1) are reliably made aware of the security tasks they need to perform; (2) are able to figure out how to successfully perform those tasks; (3) don't make dangerous errors; and (4) are sufficiently comfortable with the interface to continue using it." In other words, Usable security mechanisms are set of sophisticated and smart techniques and methods of security that are planned, designed, and developed in usable ways for genuine biometrics authentication users, and unusable for adversaries [6]. Next section provides some guidelines for planning and designing usable security for biometric Authentication.

5 Usable security for biometric authentication

Based on the definition of "usable security" on the previous section and recalling the areas of usability security overlap, usable security guidelines should be followed to integrate the concepts of both usability and security. In his PhD thesis [15], Simson Garfinkel collected six usable security principles and used them to come up with usable security patterns. In [15], Andrei Ferreira and his co-authors proved that Garfinkel's patterns can be used as guidance for software developers to build such usable security

mechanisms. We consider Garfinkel's patterns as the best to be followed to apply the real meaning of usable security on biometrics authentication systems. To summarize, here are the guidelines listed as follow: (1) Considering user-centered design as the most important, user questionnaires must be conducted on user's knowledge about biometrics, motivation to use biometrics; (2) Make the security part of the biometric user interface portable to usability alternatives. In other words, biometric user interface can provide multiple traits sensors (for instance, fingerprints, face, and voice), and let the user to choose the trait he/she likes. If only fingerprint is used as a trait, let the user to choose whichever finger he/she likes. (3) Exception handling process must be as automated as possible, and the least to be used. Multiple traditional authentication mechanisms (like ID cards and passwords) are used in limited cases to automate exception processes.

At the of this detailed explanation about using biometrics for usability security alignment, smartphones' adoption of using biometrics for authentication would be one of the best examples nowadays that the above three recommended guidelines are adequately and properly used for. Smartphone companies developed biometric-based authentication systems according to the user-centered design principles [18].

Increasingly, many smartphone companies provide alternative biometric traits for the user from which to choose in order to increase authentication systems usability [19]. Moreover, in the case that biometrics-based systems don't work properly and become not usability facilitator, the authentication systems directly automate using traditional methods such as passwords and/or PINs to complete the authentication process and grant access to the legitimate users.

6 Conclusion

Biometrics provide reliable alternative methods of authentication that fit in many cases. However, in order to get the optimal benefits and utilize biometrics for successful authentication, proper usability application should be considered. This work determined the areas where conflict of interest between security and usability may accrue during biometrics authentication process, as such areas are core to usable-security research work. Further research on usable-security biometric-based authentication should focus on those areas, which will be the future direction for this article.

REFERENCES

[1]. Mayron, L. M and Hausawi, Y and Bahr, G. S., “Secure, usable biometric authentication systems, International Conference on Universal Access in Human-Computer Interaction, Springer, p. 195—204 (2013)

[2]. Toledano, D.T. and Fernndez Pozo, R. and Hernndez Trapote, and Hernndez Gmez, L, “Usability evaluation of multi-modal biometric verification systems”, Interacting with Computers, v. 18, no. 5, Elsevier, p. 1101--1122, (2006)

[3]. Al-Harby, F. and Qahwaji, R. and Kamala, M., “UsersÕ Acceptance of Secure Biometrics Authentication System: Reliability and Validate of an Extended UTAUT Model”, Networked Digital Technologies, Springer, p. 254—258 (2010)

[4]. Jain, A.K. and Ross, A.A. and Nandakumar, K., “Introduction to biometrics “, Springer (2011)

[5]. Braz, C. and Robert, J.M., “Security and usability: the case of the user authentication methods”, Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine, ACM, p. 199—203 (2006)

[6]. Cranor, L.F. and Garfinkel, S, “Guest Editors' Introduction: Secure or Usable? “, Security and Privacy, IEEE, v. 2, no. 5, p. 16—18, (2004)

[7]. Kumar, N, “Password in practice: a usability study”, Journal of Global Research in Computer Science, v. 2, no. 5, p. 107--112, (2011)

[8]. Sasse, M.A. and Brostoff, S. and Weirich, D, “Transforming the Ôweakest linkÕÑa human-computer interaction approach to usable and effective security”, BT technology journal, Springer, v. 19, no. 3, p. 122--131, (2001)

[9]. Riley, C. and Buckner, K. and Johnson, G. and Benyon, D, “Culture \& biometrics: regional differences in the perception of biometric authentication technologies”, AI and society, v. 24, no. 3, Springer, p. 295--306, (2009)

[10]. Fernandez-Saavedra, B. and Alonso-Moreno, R. and Uriarte-Antonio, J. and Sanchez-Reillo, R, “Evaluation methodology for analyzing usability factors in biometrics “, Aerospace and Electronic Systems Magazine, IEEE, v. 25, no. 8, p. 20—31, (2010)

[11]. Kukula, E.P. and Sutton, M.J. and Elliott, S.J, “The Human-Biometric-Sensor Interaction Evaluation Method: Biometric Performance and Usability Measurements”, Instrumentation and Measurement, IEEE Transactions on, v. 59, no. 4, p. 784--791, (2010)

[12]. Hausawi, Y. M,. "Towards a Usable-Security Engineering Framework for Enhancing Software Development" Florida Institute of Technology (2015)

[13]. Sasse, M.A, “Computer security: Anatomy of a usability disaster, and a plan for recovery”, Proceedings of CHI 2003 Workshop on HCI and Security Systems, Citeseer (2003)

[14]. Patrick, A.S, “Usability and acceptability of biometric security systems”, Lecture Notes in Computer Science, SPRINGER-VERLAG, p. 105--105, (2004)

[15]. Garfinkel, S, “Design principles and patterns for computer systems that are simultaneously secure and usable” Massachusetts Institute of Technology (2005)

[16]. Ferreira, A. and Rusu, C. and Roncagliolo, S, “Usability and security patterns “, Advances in Compu ter-Human Interactions, 2009. ACHI'09. Second International Conferences on IEEE, p. 301--305, (2009)

[17]. Whitten, A. and Tygar, J.D, “Why Johnny canÕt encrypt: A usability evaluation of PGP 5.0”, Proceedings of the 8th USENIX Security Symposium,McGraw-Hill, v. 99 , (1999)

[18]. Van Der Geest, Thea M and Buimer, Hendrik P, “User-centered priority setting for accessible devices and applications”, Mensch \& Computer Workshop band , (2015)

[19]. Mahfouz, Ahmed and Mahmoud, Tarek M and Eldin, Ahmed Sharaf, “A survey on behavioral biometric authentication on smartphones”, Journal of information security and applications , (2017)