Choice-Based Authentication: A Usable-Security Approach

Yasser M. Hausawi, William H. Allen, and Gisela Susanne Bahr

Department of Computer Sciences
Florida Institute of Technology
Melbourne, FL 32901, USA
{yhausawi@my., wallen@, gbahr@}fit.edu

Abstract. Authentication is an important security component of almost any software application. It serves as the application's security front door by controlling access with the goal of protecting the confidentiality and integrity of the system. However, with the large variety of software applications that an end user interacts with daily, authentication is becoming a usability issue that has the potential to weaken a system's overall security. The increasing complexity of dealing with a variety of authentication mechanisms often causes end users to develop negative security behaviours, such as writing down passwords. Moreover, some of the currently available authentication mechanisms, such as alphanumeric passwords, raise universal access issues due to both the issue of remembering a complex sequence of characters and the difficulty some individuals may have in entering that exact sequence on a keyboard or mobile device. This article proposes an authentication approach that seeks to address these usability, universal access, and security issues.

1 Introduction

Computing systems have become some of the most important tools for easily exploring and investigating the intricate nature of art, sciences, and engineering. Humans interact with systems on a daily basis to get their jobs done efficiently and effectively. However, with the revolution of information technology, humans tend to use these systems with both good and bad intentions. Consequently, security and usability have become two important quality attributes that need to be adjusted, integrated, and properly balanced. Usability assumes that humans interact with systems for the purposes for which they were built in order to perform an appropriate task, while security considers that humans may interact with systems with malevolent intent. Those two contradicting goals lead to a conflict of interest between the two attributes that is evident in irrational interaction design [2].

Human-Computer Interaction (HCI) specialists and security experts addressed this problem by forming a new solution field called usable-security [3]. Whitten and Tygar [26] define usable-security as a security system where users are aware of security tasks that need to be performed, able to figure out how those tasks are

C. Stephanidis and M. Antona (Eds.): UAHCI/HCII 2014, Part I, LNCS 8513, pp. 114–124, 2014.

properly performed, do not make harmful errors, and are comfortable with the interface. Usable-security has become a new hybrid software quality attribute with the goal of making security and usability synergistic rather than dissonant [9,11,22,25]. To this end, HCI and security experts have provided various approaches and design techniques to merge, align, and integrate usable-security, such as: user-centered interface design [5], early involvement of both security and usability [8], designation design [27], user decision-based security information [24], filtering users and transmitted data [15], using biometrics [14], using principles and patterns [9], and incorporating post-hoc security layers [10].

Authentication is one area that illustrates the security-usability conflict of interest [19]. Kumar [14] concluded that alphanumeric-password-based authentication cannot be both usable and secure at the same time and suggested graphical passwords and biometrics as alternatives to alphanumeric passwords. In contrast, Sasse et al. [23] concluded that alphanumeric passwords are not usable because usability is not considered as a fundamental security requirement.

This article proposes an authentication system that addresses usability, universal access, and security issues based on two concepts. The first concept is to allow end users to select their authentication method based on their preferences in order to provide better usability and universal access, and the second concept is to increase the difficulty for adversaries by displaying all of the possible authentication methods at one time, increasing the complexity of guessing the user's chosen authentication approach.

The next section presents background information about security, usability, usable-security, and Universal Access. Section 3 introduces our Choice-Based Authentication Approach (CBAA) along with a demonstration to the approach. Section 4 describes an informal heuristic analysis. Section 5 discusses the results of the heuristic evaluation, and Section 6 concludes this article.

2 Background

The CBAA involves two main areas in general, namely: usability and security. In addition, universal access and authentication are particularly involved. In the following, some background information is provided about the involved areas.

2.1 Security

Security is a set of related methods and techniques used together as one mechanism to protect computer systems from being negatively impacted by both legitimate users and adversaries. Any computer system has weaknesses that can be exploited to harm the system itself, its users, or its owners. As of today, there is no computer system that can be perfectly secured nor a security mechanism that can make other systems fully secure [9]. Pfleeger and Pfleeger define computer security as "preventing the weaknesses from being exploited and understanding preventive measures that make the most sense" [20]. By making the weaknesses more difficult to exploit, an acceptable degree of security may be achieved and

a system's behavior can be controlled. Security researchers attempt to provide mechanisms that are reliable and cause secured systems to behave as expected. As stated by Garfinkel and Spafford: "a computer is secure if you can depend on it and its software to behave as you expect it to" [9]. To meet the above definitions, there are three primary security properties: confidentiality, integrity, and availability. Confidentiality involves restricting a system and its information so that it is only accessible to legitimate users. Integrity ensures that the alteration of system's behavior and its information is only done in an appropriate way. Availability assures that the system, its information and other resources are accessible whenever needed.

Among the above three properties, confidentiality has been the subject of considerable security research, thus many security methods and techniques have been developed to ensure confidentiality, such as authentication and access control [4,20]. Authentication is a security process that verifies an individual's identity upon access request. Access control is another security process that manages what an user can access based on policies or on a user's roles [4]. The scope of this work is limited to the authentication process. Therefore, some background information about authentication is provided here.

There are three common authentication approaches: *what an individual knows*, such as passwords, *what an individual has*, such as ID cards, and *who an individual is*, such as biometrics. The first two approaches are more traditional, while the third approach has emerged more recently. All three approaches have advantages and disadvantages (see Table 1). On one hand, the traditional authentication approaches are prone to memorability, theft and loss problems. The more modern biometric authentication is prone to privacy problems because it uses individuals' private traits that cannot be returned or changed by the individuals after they are taken. Moreover, the newer approach has not yet proven to be as reliable as the others. On the other hand, all three approaches have advantages. The traditional approaches can verify authentication methods with a high degree of accuracy, however, they cannot identify the authentication method's user. The modern approach (biometrics) can identify individuals, but cannot provide 100% accuracy.

2.2 Usability

The International Standard Organization (*ISO*) defines usability as the individuals' ability to perform a particular task effectively, efficiently, and with an accepted degree of satisfaction [12]. The ISO definition summaries a complete usability engineering process. The definition has three primary usability properties that need to be met, namely: effectiveness, efficiency, and satisfaction. Effectiveness is a product's ability to help individuals to perform a particular task successfully with a lowest number of errors. Efficiency is a product's ability to help individuals to perform a particular task effectively and within an acceptable amount of time. Satisfaction is a products ability to help individuals to perform a particular task effectively and efficiently along with an acceptable degrees of easiness, happiness, and confidence. Moreover, there are secondary properties that

Table 1. Advantages and Disadvantages of Primary Authentication Approaches

Category	**Traditional**		**Modern**
Approach	*What individuals know*	*What individuals have*	*Who individuals are*
Methods	Passwords, PINs	IDs, Tokens	Biometrics
Memory Problems	Major	Minor	Minor
Theft Problems	Major	Major	Minor
Loss Problems	Major	Major	Minor
Privacy Concerns	Moderate	Moderate	High
Matching Accuracy	High	High	Medium
Verification	Yes	Yes	Yes
Identification	No	No	Yes
Cost	Low	Medium	High
User Acceptance	Moderate	Moderate	Moderate
Universal Access	Moderate	Moderate	Moderate

have both direct and indirect impact on the three primary properties. These properties are: memorability, learnability, accuracy, and users' knowledge.

2.3 Usable-Security and Universal Access

Whitten and Tygar [26] define usable-security as a security system where users are aware of security tasks that need to be performed, are able to figure out how those tasks are properly performed, do not make harmful errors, and are comfortable with the interface. Universal Access is defined as set of techniques and methods that "seek to provide the utility of modern information technology to as broad a range of individuals as possible" [16]. Consequently, usable-security and Universal Access can be jointly defined as: a security system that can be utilized by as broad a range of individuals as possible where those individuals are aware of security tasks that need to be performed, able to figure out how those tasks are properly performed, do not make harmful errors, and are comfortable with the interface. It becomes obvious that usability is essential to Universal Access to provide universal usability for software products [16]. Moreover, usability has direct impact on a security mechanism's success through providing usable-security. From the above observations we can conclude that in order to develop a system that provides both security and Universal Access, usability must be highly considered [16].

3 Choice-Based Authentication Approach

Typical authentication systems provide one method for verifying users (passwords, ID cards, tokens, or biometrics) [13]. In some advanced authentication systems, two-factor authentication is used to verify users. Two-factor authentication is a methodology that uses two different factors, such as combining

passwords, tokens or biometrics together to authenticate individuals [13]. However, the user still does not have the option to select the most suitable method of interaction with the system. It appears that two-factor authentication increases the complexity of security systems enough to make penetration more difficult [3]. This observation prompts two questions: **Is increased computational complexity necessary to make authentication systems difficult to penetrate?** and **Is there a simpler way to make security systems simultaneously usable and difficult to penetrate rather than simply adding complexity?** [10] To address the above concerns, we propose a Choice-Based Authentication Approach (CBAA) as a way to make security and usability synergistic to achieve an acceptable level of usable-security without increasing users' cognitive load.

The approach is based on two concepts. The first concept is allowing end users to select their authentication method for better usability in order to decrease users' cognitive load and increase their desire to cooperate with the system. In addition, this concept supports increasing universal access because it allows users to select from a group of authentication approaches that are most suitable for a broad range of users [16]. The second concept is increasing the difficulty for adversaries by displaying all of the possible authentication methods during the login process. The goal of this work is not to produce a novel authentication method, but rather to demonstrate that it is possible to employ currently available authentication technologies in a way that is both more secure and more usable.

3.1 CBAA Demonstration

Figures 1 and 2 show an authentication system that is based on the CBAA approach. The system uses three different authentication methods, namely: alphanumeric password based on the NIST SP 800 Series [6], graphical password based on the recall-based method [7,21], and fingerprint biometrics [1,13,16,25]. The purpose of the CBAA demonstration is to investigate whether usable-security can be achieved by giving end-users the freedom to select the authentication method they prefer. Each of the three authentication methods will be described in details as follows.

Alphanumeric Password. For the purposes of this demonstration, we derived a simplified password creation policy that was adapted from the password strength guidelines provided by the National Institute of Standards and Technology (NIST SP 800 Series) [6]. The justification for lowering the standard for this paper is to reduce the cognitive load for password creation so that it was more in line with the other techniques. However, for a real system, both the password and graphical authentication methods should have stronger requirements. The guidelines used for this paper consist of the following policy points:

1. The length of the password must be at least eight characters.
2. Must contain at least one digit (number).

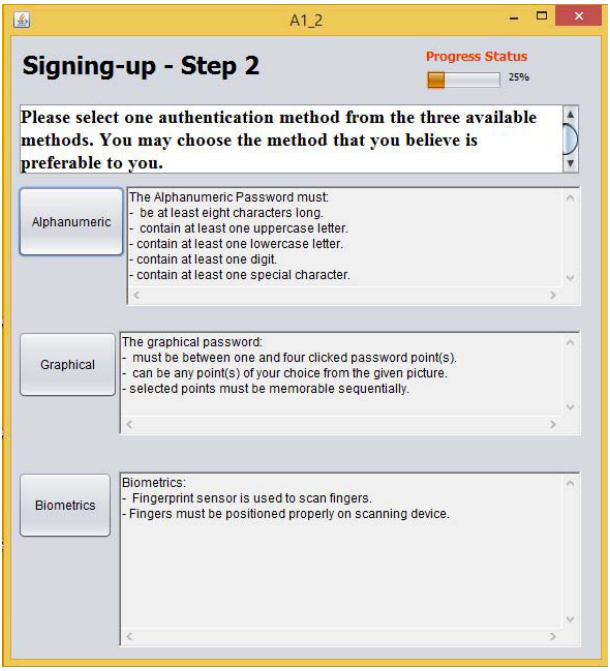

Fig. 1. A snapshot of the CBAA signing-up window that works towards usability

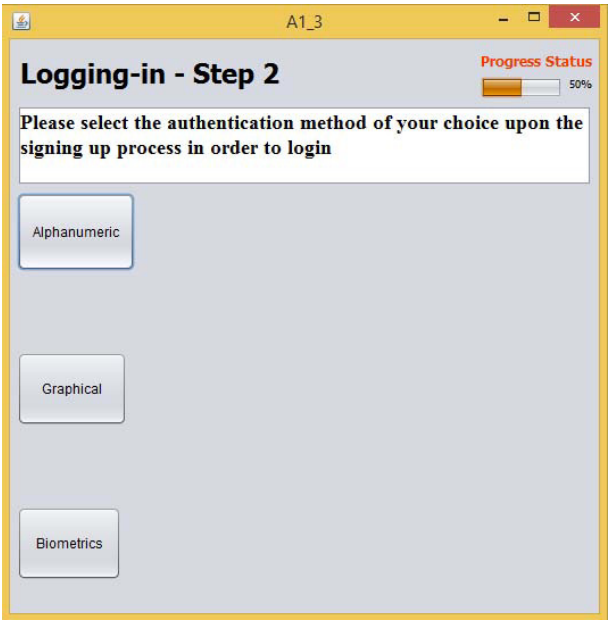

Fig. 2. A snapshot of the CBAA logging-in window that works towards security

3. Must contain at least one special character.
4. Must contain at least one capital letter.
5. Must contain at least one lower letter.

Graphical Password. There are two main approaches for graphical passwords [7,21] namely: recognition based and recall based. The recognition based approach relies on already created and displayed grids or objects that users select as passwords. The recall based approach has the user select specific points from a picture that is provided. The experiment in this paper employs the second approach because it is more secure than the recognition based approach against many attacks, such as shoulder surfing and social engineering [21]. Recall based graphical passwords are also more difficult to guess than with the recognition based approach [7]. However, as described above, this experiment is concerned with user choices and so the security policy it uses for graphical passwords is less secure than should be used in real systems. Subjects who choose to use graphical authentication are provided with a picture and are asked to select points on the image, based on the following guidelines:

1. The number of points chosen must be between one and four.
2. It can use point(s) from anywhere in the given picture.
3. It must be recalled in the same sequence as it was chosen.

Biometrics. There are many biometric traits available for authentication, such as face, fingerprint, voice, iris, signature, gait, hand geometry, palm-print, and soft biometrics [13,16]. Fingerprints are the most popular biometric trait that can easily be extracted in a controlled environment such as for lab experiments [1,25]. The subjects who choose biometrics as an authentication method are provided with a commercially-available fingerprint sensor to scan their fingerprints.

4 Heuristic Analysis and Evaluation

Although the ultimate goal of this research is to conduct controlled experiments with a wide range of users, we first chose to investigate the effectiveness of our proposed approach by conducting an informal usable-security heuristic evaluation. Heuristic evaluation is a critique-based expertise and heuristic feedback investigation that is performed by security and usability experts. There are four main advantages of conducting this type of evaluation [18]: 1) identifying minor issues to resolve them before involving end users, so formal experiments focus on major design issues, 2) enhancing the design through getting new improvement ideas that may be presented by the evaluators before conducting the official experiment, 3) providing indicative data that helps in identifying the possible directions and potential success of running formal experiments, and 4) helping to smooth off the rough edges.

Our informal usable-security heuristic evaluation for the demonstration of the proposed CBAA depends on checking the CBAA-based demonstration system's

compliance with the heuristic usability principles of Jakob Nielsen [17]. Moreover, the usable-security principles of Simson Garfinkle [9] were added to the list of the principles. The informal evaluation was done with several individuals. Each expert walked through the demonstration twice and went over all of the tasks during each run. Seven persons participated in the heuristic evaluation, five males and two females. Their security and usability experience is between one and over 20 years. The following list represents the heuristics used for evaluating the demonstration:

- H_1 : **Visibility of System Status:** The system provides feedback on the status of performed.
- H_2 : **Match between System & World:** The system speaks the users' language (meaningful vocabulary, phrases, and concepts).
- H_3 : **User Control & Freedom:** The system provides the choice of "exit" at any time.
- H_4 : **Design Consistency & Security Standards:** The system provides enough consistency on flow control and objects placement, and follow standard Policies.
- H_5 : **Error Prevention:** The system itself encourages error avoidance by controlling the process flow.
- H_6 : **Recognition Support:** The system supports recognition though minimizing recall (minimizing cognitive load).
- H_7 : **Flexibility & Efficiency of Use:** The system allows skipping unnecessary or known steps (shortcut) to save time.
- H_8 : **Aesthetic & Minimalist Design:** The system provides only relevant information for each dialog.
- H_9 : **Help Users Recognize, Diagnose, and Recover from Errors:** The system provides error messages that indicate the problems and suggest proper solutions.
- H_{10} : **Help & Documentation:** The system provides instant and informative help.
- H_{11} : **Least Surprise & Astonishment:** The system avoids surprising and astonishing users with unexpected information or actions.
- H_{12} : **Good Security Now:** The system adopts up-to-date security techniques.
- H_{13} : **No External Burden:** The system avoid affecting other systems and applications negatively.

5 Results and Discussion

Results of the heuristic evaluation are displayed in Figure 3. The heuristic evaluation levels are ranged between 6.7 and 9.3 with an overall average evaluation level of 8.1.

Both H_2 and H_{12} received the highest evaluation level (9.3). This indicates that the CBAA system uses meaningful vocabulary, phrases, and concepts that

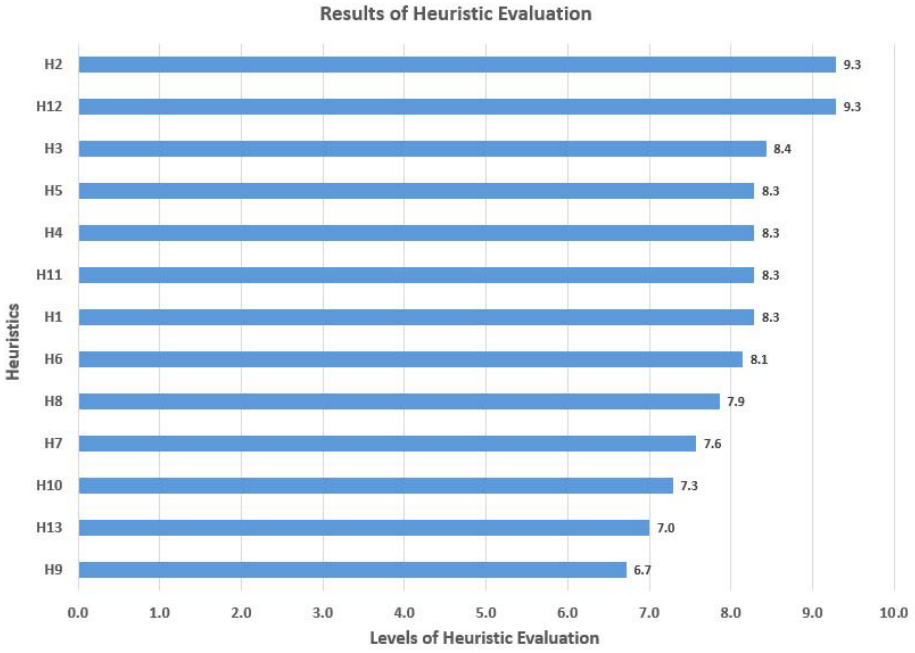

Fig. 3. The Results of Heuristic evaluation

speak end users' language. Moreover, the system adapts up-to-date security techniques through using graphical passwords and biometrics (fingerprints). H_1, H_3, H_4, H_5, and H_{11} were evaluated at levels between 8.4 and 8.1, which indicates that the system provides feedback on the status of user's progress. Moreover, it allows users to exit at any time, provides consistent flow control and object placement of the design along with following the standard authentication policies, encourages error avoidance by controlling the process flow, avoids unexpected information and/or actions. However, these points could be enhanced more. The rest of the heuristic points (i.e. H_6, H_7, H_8, H_9, H_{10}, and H_{13}) were evaluated at levels below 8, which indicates that more work is needed to enhance the usable-security of the proposed system through improving these heuristics. We concluded that the system should be enhanced in the following ways:

- Helping end users to recognize the authentication processes without having to recall much information or need experience to interact with the proposed authentication approach.
- Allowing end users to skip unnecessary steps through providing shortcuts, so users can move to the other authentication methods at any time.
- Focusing on only providing relevant information for each dialog.
- Supporting end users with helpful error messages that clearly explain the error and suggest solutions.
- Providing adequate help and documentation.

After analyzing the results of the heuristic evaluation, we revised the demonstration version of the CBAA to address the usability and security points that were shown to need further enhancement. The latest version of the interface will be used for future usable-security research that compares usable-security level between the proposed CBAA and the currently available standard-based authentication systems, to determine whether the CBAA that we proposed provides better usable-security than the authentication systems that are currently available. A full-scale survey of a wide range of users is planned and the results will be submitted for publication in the future.

6 Conclusion

We proposed a Choice-Based Authentication Approach (CBAA) that is based on two concepts: end-users' preference of authentication method to address usability and universal access concerns, and improved security by raising the bar for adversaries. Future work will focus on investigating whether this approach provides better usable-security than the standard single-authentication approach, as more work is needed to determine how responsive this approach is to end-users with differing levels of security experience.

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.) NDT 2010. CCIS, vol. 87, pp. 254–258. Springer, Heidelberg (2010)
2. Bahr, G.S., Allen, W.H.: Rational interfaces for effective security software: Polite interaction guidelines for secondary tasks. In: Stephanidis, C., Antona, M. (eds.) UAHCI 2013, Part I. LNCS, vol. 8009, pp. 165–174. Springer, Heidelberg (2013)
3. Balfanz, D., Durfee, G., Smetters, D.K., Grinter, R.E.: In search of usable security: Five lessons from the field. IEEE Security & Privacy 2(5), 19–24 (2004)
4. Bertino, E., Martino, L., Paci, F., Squicciarini, A.: Security for Web Services and Service-Oriented Architectures. Springer Publishing Company (2009) (Incorporated)
5. Braz, C., Robert, J.-M.: 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)
6. Burr, W.E., Dodson, D.F., Newton, E.M., Perlner, R.A., Polk, W.T., Gupta, S., Nabbus, E.A.: Sp 800-63-1. electronic authentication guideline (2011)
7. Dirik, A.E., Memon, N., Birget, J.C.: Modeling user choice in the passpoints graphical password scheme. In: Proceedings of the 3rd Symposium on Usable Privacy and Security, pp. 20–28. ACM (2007)
8. Flechais, I., Mascolo, C., Sasse, M.A.: Integrating security and usability into the requirements and design process. International Journal of Electronic Security and Digital Forensics 1(1), 12–26 (2007)
9. Garfinkel, S.: Design Principles and Patterns for Computer Systems that are Simultaneously Secure and Usable. Ph.D. thesis, Massachusetts Institute of Technology (2005)

10. Gutmann, P., Grigg, I.: Security usability. IEEE Security & Privacy 3(4), 56–58 (2005)
11. Hausawi, Y.M., Mayron, L.M.: Towards usable and secure natural language processing systems. In: HCI International 2013 Extended Abstracts, pp. 109–113. Springer (2013)
12. ISO, W.: 9241-11. ergonomic requirements for office work with visual display terminals (VDTs). The international organization for standardization (1998)
13. Jain, A.K., Ross, A.A.A., Nandakumar, K.: Introduction to biometrics. Springer (2011)
14. Kumar, N.: Password in practice: An usability survey. Journal of Global Research in Computer Science 2(5), 107–112 (2011)
15. Lampson, B.: Privacy and security usable security: How to get it. Communications of the ACM 52(11), 25–27 (2009)
16. 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)
17. Nielsen, J.: Heuristic evaluation. Usability inspection methods 17, 25–62 (1994)
18. Nielsen, J.: How to conduct a heuristic evaluation (2001) (retrieved November 10)
19. Payne, B.D., Edwards, W.K.: A brief introduction to usable security. IEEE Internet Computing 12(3), 13–21 (2008)
20. Pfleeger, C.P., Pfleeger, S.L.: Security in Computing. Prentice Hall PTR (2006)
21. Sarohi, H.K., Khan, F.U.: Graphical password authentication schemes: Current status and key issues (2013)
22. Sasse, M.A.: 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)
23. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the weakest link a human/computer interaction approach to usable and effective security. BT Technology Journal 19(3), 122–131 (2001)
24. Stoll, J., Tashman, C.S., Edwards, W.K., Spafford, K.: Sesame: Informing user security decisions with system visualization. In: Proceedings of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems, pp. 1045–1054. ACM (2008)
25. Toledano, D.T., Pozo, R.F., Trapote, Á.H., Gómez, L.H.: Usability evaluation of multi-modal biometric verification systems. Interacting with Computers 18(5), 1101–1122 (2006)
26. Whitten, A., Tygar, J.D.: Why johnny cant encrypt: A usability evaluation of pgp 5.0. In: Proceedings of the 8th USENIX Security Symposium, vol. 99, McGraw-Hill (1999)
27. Yee, K.-P.: Aligning security and usability. IEEE Security & Privacy 2(5), 48–55 (2004)