An Integration of Usable Security and User Authentication into the ISO 9241-210 and ISO/IEC 25010:2011

Paulo Realpe-Muñoz[1(✉)], Cesar A. Collazos[1], Julio Hurtado[1], Toni Granollers[2], and Jaime Velasco-Medina[3]

[1] IDIS Research Group, University of Cauca, Popayán, Cauca, Colombia
{prealpe,ccollazo,jhurtado}@unicauca.edu.co
[2] GRIHO Research Group, University of Lleida, Lleida, Spain
antoni.granollers@udl.cat
[3] Bionanoelectronics Research Group, University of Valle, Cali, Valle del Cauca, Colombia
jaime.velasco@correounivalle.edu.co

Abstract. Currently, computer security is one of the most important tasks. However, although there are works on the interfaces design secure and usable, it is necessary to perform an investigation to integrate these two attributes in a more easy way. Security problems for computer systems include vulnerabilities because they are hard to use and have poor user interfaces due to security constraints. Nowadays, finding a good trade-off between security and usability is a challenge, mainly for user authentication services. This paper presents an integration between the ISO 9241-210 standard to find a development process and a tool for evaluating qualitative and quantitatively usable security and user authentication, taking into account some aspects, attributes and characteristics of the ISO/IEC 25010:2011 allowing that the design requirements and its heuristic evaluation are suitable for the system.

Keywords: Usable security · Authentication · Attributes · Principles · Standards · Guidelines

1 Introduction

Computer security is the area of computer science in charge of the confidentiality and integrity of the systems and data. Most current applications have incorporated security features and privacy. However, security is generally a secondary goal for most users because it is complex to use. As a result of the above, wrong decisions are taken according to security, and therefore, important information is at risk. Usable Security (USec) is the field that investigates these issues, focusing on the design of security and privacy features that are easy to use [1].

Most applications, such as, e-commerce or e-banking, need to know the identity of the users. Knowing users identity, these applications allow to provide

T. Tryfonas (Ed.): HAS 2016, LNCS 9750, pp. 65–76, 2016.
DOI: 10.1007/978-3-319-39381-0_7

permissions to access their data. This access can be provided by authentication methods which could verify the identity of users. Although security and usability are essential in the authentication process as well, the requirements for having an appropriate level of security for authentication while maintaining its usability, could generate conflict with each other.

In literature has been conducted some research on usable security and user authentication, although a large number of research works have been made for computer security [2]. This is because the integration of HCI methods with security information methods is not straightforward, due to security addresses very complex cases without benefiting the use of an application. Therefore, finding a good trade-off between security and usability is always a challenge.

We believe that one way to strike a balance between usability and security, could come integrating international standards widely recognized by the academic and business community such as ISO 9241-210 and ISO/IEC 25010:2011 into USec and user authentication.

The standard ISO 9241-210 [3] is a framework for human-centered design processes that integrates different design and development appropriate in a particular context, complementing existing design methodologies. The ISO/IEC 25010:2011 SQuaRE (Systems and Software Quality Requirements and Evaluation) (ISO/IEC 25010:2011) [4] is the standard that defines the system and software quality, which is highly focused on system's quality of use.

However, to the best of our knowledge, there is no a process, qualitative and quantitative, that describes how to develop and validate systems taking into account the design requirements and principles (also called heuristics) allowing a good trade-off between security and usability, that is, a user-centered design process for usable security and user authentication. In addition, there is no a relationship between the attributes and characteristics of the standard ISO/IEC 25010:2011 that the community can use to evaluate security and usability, assuring that the user achieves a suitable experience for a website/application.

This paper presents an integration between the standard ISO 9241-210 to find a development process and a tool for evaluating qualitative and quantitatively usable security and user authentication, taking into account some aspects, attributes and characteristics of the standard ISO/IEC 25010:2011 allowing that the design requirements and its heuristic evaluation are suitable for the system.

The main contributions of this paper are: (1) an exhaustive literature review in order to obtain principles or heuristics for systems that require security and usability, (2) a heuristic development and evaluation (quantitative and qualitative) for usable security and authentication methods according to the standard ISO 9241-210, (3) the first set of principles for USec and user authentication, taking into account some attributes and characteristics of the standard ISO 25010:2011 (which defines the software quality), and finally, (4) we propose a level of importance for each principle obtained above.

This paper is organized as follows: Sect. 2 discusses related works. Section 3 presents the human-centered design. Section 4 shows an integration between ISO 9241-210 standard and a heuristic development for USec and user authentication.

Section 5 presents the specification of USec and user authentication through quality attributes. Finally, Sect. 6 we make our conclusions and future work.

2 Related Works

Some works have suggested processes that enable to develop principles and guidelines for specific or general purposes. Yeratziotis et al. [1] present a framework within the context of online social networks that are particular to the health domain. This framework has three components: process to develop USec heuristics, heuristic evaluation and a validation process. Wilson [5] presents a process for creating useful and usable heuristics, mainly focusing the user-centered design.

Sim et al. [6] propose a design approach based on evidence for developing specific heuristics. Mujinga et al. [7] define a model for developing heuristics taking into account the security and usability for e-banking applications. This model has the disadvantage does not have a real validation by experts and users. Shneiderman et al. [8] present a set of guidelines to assist in the creation of web sites. These guidelines are particularly relevant to the design of information-oriented sites, but can be applied across the wide spectrum of web sites.

Vidal et al. [9] present an application that use the human-centered design approach for interactive systems following the process defined by the ISO 9241-210 standard. Fidas et al. [10] apply the user-centered design approach to CAPTCHA mechanisms take into account the ISO 9241-210 standard.

In 2011, ISO announced the new standard for software product quality ISO-IEC 25010:2011 [4]. SQuaRE is the term that refers to the standard that defines the system and software quality. The difference with existing standard is software security and is defined as a quality characteristic. With this product model, to evaluate security of practical system has being researched [11,12].

Zapata [13] presents the development of a consolidated model designed especially to cover the security and usability attributes of a software product. As a starting point, a new usability model on the basis of well-known quality standards and models is built. Finally, Realpe et al. [14] present a systematic review of usability principles, evaluation methods and development processes for security systems. Moreover, a research approach to integrate usability and security for user authentication systems is proposed.

3 Human-Centered Design

The purpose of user-centered design (UCD) is to develop applications with a high degree of usability. To achieve this, the user becomes the most important element in the application development process. User-centered design is based on the fundamental aim to best address the users' needs and tasks. This is the feature that lead to the design process. The needs and tasks of users must also be in line with what is stated in the requirements documents [15].

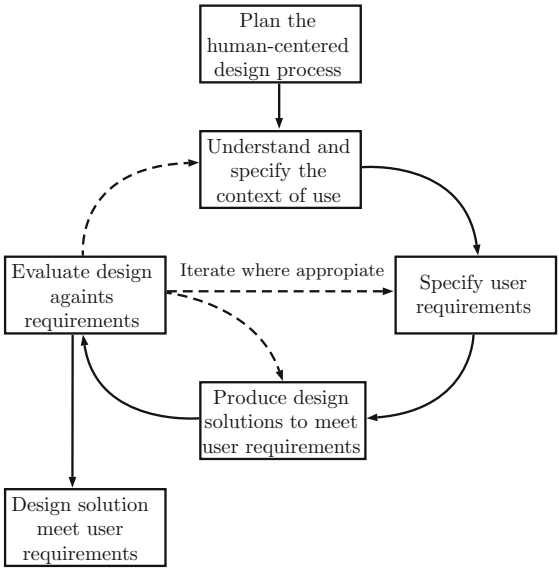


Fig. 1. Interdependence of the activities of Human-Centered Design [3]

The importance of interactive systems is reflected in the ISO 13407:1999 human-centered design for interactive systems processes, which is a guide for developing usable interactive systems incorporating the user-centered design. However, this standard was canceled and replaced by the ISO 9241-210. In this standard, the term user-centered design was replaced by human-centered design (HCD), because it addresses both stakeholders and users [9]. HCD is defined as follows: "Human-centred design is an approach to interactive systems development that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors/ergonomics, and usability knowledge and techniques" [3].

The standard ISO 9241-210:2010 provides a framework for human-centered design that integrates different design process and development appropriate in a particular context; complementing different design methodologies [9]. Figure 1 shows the activities and their interdependence defined by the standard [3].

Performing an interactive system implies that certain standards and procedures are followed by the development team. The general process defined by the standard ISO 9241-210 provides several iterations until to get all goals or requirements, they are indicated by the dotted lines [9].

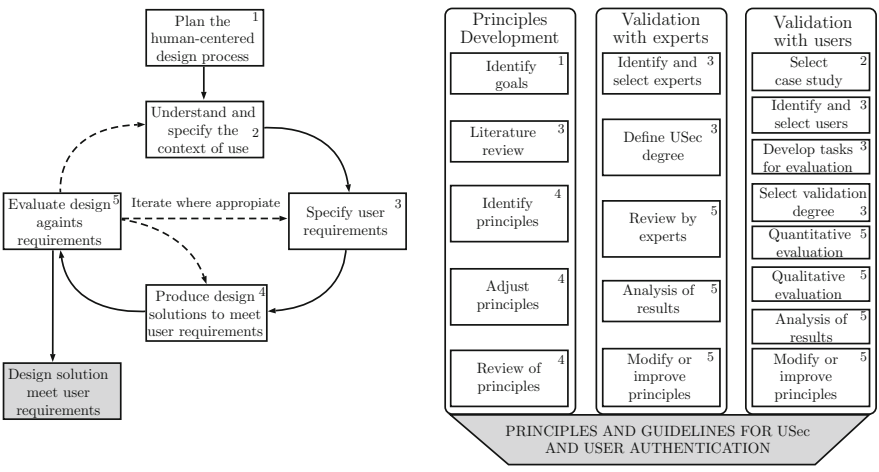
4 Integration Between ISO 9241-210 and USec Design Process

According to the works presented in Sect. 2, a development model and heuristic evaluation to usable security and user authentication which could be used in a set

wider of applications are proposed. In addition, using this model we developed the first principles set for USec and the main authentication methods (something the user knows, has and is) used by people currently. One of the important features of this model is its non-linearity: validation with experts and users can be performed independently because the results do not depend on the another one. The works presented in Sect. 2, include mainly qualitative evaluation. Our model (based on [1]) take into account quantitative and qualitative evaluation for USec and authentication methods. A complete representation of the integration between ISO 9241-210 and USec design process is presented in Fig. 2.

The process proposed is divided initially into three steps: (1) development of principles, (2) validation with experts and (3) validation with users. The first step allows to develop a set of principles for usable security and authentication methods according to literature. In the second step, the principles developed are evaluated by experts using a degree of importance. Finally, the third step, the principles must be applied in a specific context (website/application), the users perform tasks for a particular application provides us quantitative and qualitative data. The results are analyzed to improve the proposed principles.

According to the analysis of results in steps 2 and 3, the principles in step 1 could be modified or improved based on the recommendations and observations of the experts and users. At this point, the recommendations of the experts have priority due to they have knowledge and experience to determine whether the principles meet the necessary requirements. When the three steps have finished, a set of principles for usable security and user authentication is obtained. A complete representation of the process is presented in Fig. 2 b). A brief description of each step is presented as follows.



a) ISO 9241-210

b) Development Process and Validation

Fig. 2. Integration between ISO 9241-210 and development process

4.1 Principles Development (Step 1)

This step consists of 5 tasks for obtaining a set of principles preliminary.

1. **Identify Goals**: It is important to understand the purpose for developing principles or heuristics. Some goals could be: evaluate usability and security for a particular system, determine whether the system meets some quality standards, perform tasks and questionnaires to participants of the evaluation, among others.
2. **Literature Review**: A systematic literature review of principles of usability, security, privacy, user authentication, security usable and ISO / IEC standards is carried out. The study of literature is an essential requirement for knowing the requirements of the applications.
3. **Identify principles**: According to literature systematic review, the principles that might be part of the overall set (for USec and authentication methods) are identified. Each principle identified is formulated as a question, a brief explanation or examples to each question is carried out and the bibliographical sources are presented.
4. **Adjust principles**: According to the principles identified for USec and user authentication, they could be adapted to the corresponding quality attribute or characteristic (i.e. usability, security, accessibility, performance, reliability or operability). Other principles can be identified from some requirement presented in literature.
5. **Review of principles**: The review of the principles helps to place it in the appropriate attribute or characteristic. In addition, the wording is revised in order to modify or improve the question and explanation.

4.2 Validation with Experts (Step 2)

This step consists of four tasks, where experts on information security and human-computer interaction (HCI) review thoroughly the principles obtained. The experts give recommendations for improving the principles.

1. **Identify and select experts**: The experts should have knowledge and experience in areas of HCI and information security. This allows that the principles have credibility and validity.
2. **Define USec degree**: The USec degree represents the importance of each principle. To choose this degree of importance, a set of levels of importance is proposed, following the criteria of accessibility levels in W3C[1] (World Wide Web Consortium).
   (a) **S degree**: the principles of the S degree are **vital** to avoid security and usability breaches of the system and to assure that the user achieves a suitable experience.
   (b) **SS degree**: the principles of the SS degree are **important** to avoid security and usability breaches of the system and to assure that the user achieves a suitable experience.

[1] http://www.w3.org/TR/WAI-WEBCONTENT/.

   (c) **SSS degree**: it is **advisable** to consider the principles of the SSS degree to avoid security and usability breaches of the system and to assure that the user achieves a suitable experience.
3. **Review by experts**: The experts evaluate the principles (according to the previous classification) using some kind of tool (e.g., MS Excel) and they evaluate the level of importance for each principle. In addition, they give general recommendations and for each principle.
4. **Analysis of results**: From the results, the analysis of results and conclusions are made.
5. **Modify or improve principles**: From the above analysis, the principles set may be modified or improved.

4.3 Validation with Users (Step 3)

This step consists of eight tasks where a group of users develop different activities, including the case study for validating.

1. **Select case study**: In this step, it is necessary to establish criteria (application domain, real scope, type of users, among others) in order to identify the website/application for validating security and usability. In this case, it is necessary to perform a procedure to determine the website/application for evaluating.
2. **Identify and select users**: Once the case study has been identified and selected, users are selected. There are no criteria for selecting the users. Preferably, one would approach potential users of the website/application.
3. **Develop tasks for evaluation**: The goals of the evaluation are described and the tasks that users make during their interaction with the website or application are developed.
4. **Select validation degree**: In this case, the degree of validation for users corresponds to a type previously established scale. Initially, a Likert scale is used.
5. **Quantitative evaluation**: Once users have been identified and the tasks have been developed, the case study is assessed quantitatively. For an authentication method, the evaluation quantitative could be authentication time, ease of learning, deep-processing and error probability. When finished, users complete a user satisfaction questionnaire.
6. **Qualitative evaluation**: Users (experts in HCI and security information) qualitatively assess the application using the principles of step 1 for USec and authentication methods. Finally, a questionnaire is developed in order to obtain recommendations.
7. **Analysis of results**: From the results, the analysis of results and conclusions are made.
8. **Modify or improve principles**: From the above analysis, the principles set may be modified or improved.

5 Specification of USec and User Authentication Through Quality Attributes

SQuaRE - ISO/IEC 25010:2011 [4] is a standard that defines the software quality system. However, there is no relationship between some attributes and characteristics of this standard and the principles of USec and authentication methods that the community can use for evaluating website and applications. To achieve this, some aspects of literature according to USec and authentication taking into account the ISO/IEC 25010:2011 should be considered.

From the systematic literature review, the works that might be part of the heuristic overall set (for USec and authentication methods) are: Ibrahim et al. [16], Nurse et al. [17], Katsabas et al. [18], Yeratziotis et al. [1], Mijinga et al. Mujinga2013, Bonastre et al. [19], Cranor et al. [20], Johnston et al. [21] among others. According to the above, the attributes and characteristics of the standard that could carry out this relation are usability, security, accessibility, reliability, operability and performance. Figure 3 is presented the relationship.

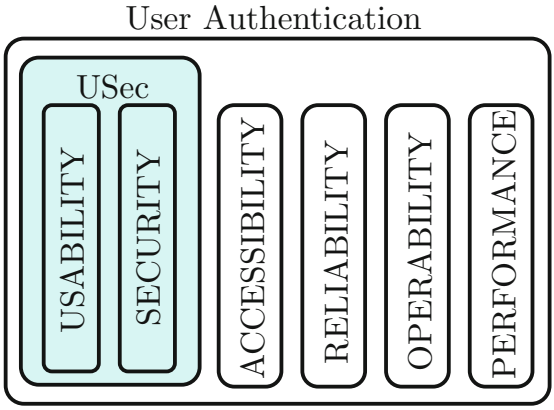


Fig. 3. Attributes for USec and user authentication

Some of these attributes have some characteristics which are included in the standard ISO/IEC 25010:2011. For security are included confidentiality, integrity, authenticity and non-repudiation. For performance are included time behaviour and minimal action. According to the systematic literature review and an exhaustive analysis, usability and security have the largest number of principles. Each principle found was analysed and located in the suitable place according to the process presented in Fig. 2. A total of 152 principles or heuristics which are distributed in specific attribute or characteristic is showed in Table 1. A brief description of each attribute or characteristic discussed above is presented as follows.

Table 1. Number of principles for each attribute

Attribute	Number of principles
Usability	75
Security	34
Accessibility	8
Performance	11
Operability	9
Reliability	15
TOTAL	**152**

1. **Usability**: based on Nielsen's 10 usability heuristics for user interface design [22], in addition, convey features are included [21]. Convey features inform the user of the available security features while the Nielsen's criterion of visibility allows the user to "see" if these features are active and being used.
2. **Security**: Our model of security according to ISO/IEC 25010:2011 have five important characteristics such as integrity, authenticity, confidentiality and non-repudiation and privacy.
3. **Operability**: It refers to the effort required to operate an authentication method.
4. **Accessibility**: Accessibility allows that everyone, regardless of cognitive, mobility and sensory skills, can use an authentication mechanism. This includes disabilities such as hearing, sight, mobility, learning and colour, which are pertinent in an authentication context. Accessibility also applies to levels of technical skills and literacy as well as the quality of the users equipment [23].
5. **Reliability**: Reliability indicates the ability to perform specific functions that allow carrying out a successful authentication. In this regard, it is also important to consider some aspects of security (integrity and confidentiality), maintenance and technical support.
6. **Performance**: For authentication methods, is taking into account two aspects [24]:
   (a) *Minimal action*: The capacity of the application to help users for achieving their tasks in a few steps.
   (b) *Time response*: It represents the time required to load the application, i.e., how fast the system responds according to the user's instructions.

As previously stated, the outcome from step 1 according to Fig. 2 is 6 attributes or characteristics and 152 principles for USec and authentication methods. Each attribute has its own set of principles that assist experts in applying the principle in practice. In Table 2 is presented an example of the principles of accessibility. In the first column, the heuristic is formulated as a question, in the second column is presented a short explanation or example of the principle and finally, the bibliographical sources of the principle are shown in the third column.

Table 2. Principles for accessibility

Principle	Comment	Source
Does the system allow to use graphical passwords to users with reading difficulties?	The images could help people to authenticate when they have reading difficulties (e.g., dyslexia)	[25]
In biometric authentication, is the system composed of standard devices?	Devices standard allow easy setting and use for users	[24]
In authentication using ownership factors, Does the server is integrated with software and hardware suitable?	Install software and hardware suitable, allow a better performance and usability for users in the authentication process	[23]
Does the system avoid using random keys in the step of registration or authentication?	Using random keys (e.g., One-Time Passwords) are difficult to use for users because it is not possible to memorize all passwords	[23]
In an authentication process, Does the system avoid extra effort?	The authentication process should be intuitive and effortless extra (e.g., cognitive or physical)	[23]
In an authentication system using inherence factors, Does the system can be configured for people with physical limitations?	People with physical limitations (e.g., dyspraxia), the system should be easily configured for these cases	[23]
Does the system provides users with alternatives to authenticate?	This could improve the availability and convenience of the system	[24]
Can the authentication method to be adapted for new and experienced users?	The authentication method should have settings options for new and experienced users	[23]

6 Conclusions and Future Work

Security is a problem area for user interface design. Consequently, developers require tools that can assist them to improve their designs in terms of usable security for websites/applications, for instance, user authentication. Security and privacy design issues can be reduced using the USec principles. This is an important contribution to the USec field.

We proposed an integration between the standard ISO 9241-210 to find a development process and a tool for evaluating qualitative and quantitatively usable security and user authentication, taking into account some aspects and attributes and characteristics of the standard ISO/IEC 25010:2011. Many users are not able to perceive the security issues correctly, generating a security threat due to misunderstanding and avoid tactics to protect the system.

Although there are different methods for evaluating the usability of security systems, these methods are not user-centered due to the lack of suitable principles. Future work will be oriented to analyze and review the heuristic set by experts in order to obtain a level of importance for each principle, in addition, examine the suggestions of the experts according to the principles set to be modified or improved.

Acknowledgement. Paulo Realpe-Muñoz thanks to Colciencias for the scholarship and to University of Lleida for the internship.

References

1. Yeratziotis, A., Greunen, D., Pottas, D.: A framework for evaluating usable security: the case of online health social networks. In: 6th International Symposium on Human Aspects of Information Security and Assurance (2012)
2. Payne, B., Edwards, W.: A Brief Introduction to Usable Security. IEEE Comput. Soc. **12**, 13–21 (2008)
3. International Standard ISO: ISO 9241–210 Ergonomics of Human-System Interaction - Part 210: Human-Centered Design for Interactive Systems. International Organization for Standardization ISO (2010)
4. International Standard ISO: ISO/IEC 25010–2011. Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models. International Organization for Standardization ISO (2011)
5. Wilson, C.: Credible Checklists and Quality Questionnaires: A User-Centered Design Method, 1st edn. Morgan Kaufmann, San Francisco (2013)
6. Sim, G., Read, J.C., Cockton, G.: Evidence based design of heuristics for computer assisted assessment. In: Gross, T., Gulliksen, J., Kotzé, P., Oestreicher, L., Palanque, P., Prates, R.O., Winckler, M. (eds.) INTERACT 2009. LNCS, vol. 5726, pp. 204–216. Springer, Heidelberg (2009)
7. Mujinga, M., Eloff, M., Kroeze, J.: Towards a heuristic model for usable and secure online banking. In: 24th Australian Conference on Information Systems (ACIS), RMIT University, pp. 1–13 (2013)
8. Shneiderman, B., Leavitt, M.: Research-Based Web Design and Usability Guidelines. US Government Printing Office, Whashington D.C. (2006)
9. Vidal, D., Ibarra, J., Flores, B., Lopez, G.: Adoption of the Standard ISO 9241–21: 2010 on construction of interactive systems based in software. In: International Conference on Research and Innovation in Software Engineering. CANISOFT (2012)
10. Fidas, C., Hussmann, H., Belk, M., Samaras, G.: iHIP: towards a user centric individual human interaction proof framework. In: CHI Extended Abstracts, pp. 2235–2240. ACM (2015)
11. Haiyun, X., Heijmans, H., Visser, J.: A practical model for rating software security. In: 7th International Conference on Software Security and Reliability-Companion (SERE-C), pp. 231–232. IEEE (2013)
12. Colombo, R., Guerra, A., Balcao, A., Caruso, C.: Prioritization of software security intangible attributes. SIGSOFT Software Engineering Notes, pp. 1–7. ACM (2012)

13. Zapata, L.: Development of a Model for Security and Usability. Master Thesis. Universidad Politecnica de Madrid (2013)
14. Realpe, P., Collazos, C., Hurtado, J., Granollers, T.: Towards an integration of usability and security for user authentication. In: 16th International Conference on HCI, pp. 43:1–43:6 (2015)
15. Leventhal, L., Barnes, J.: Usability Engineering: Process, Products and Examples. Prentice Hall, Upper Saddle River (2007)
16. Ibrahim, T., Furnell, S., Papadaki, M., Clarke, N.: Assessing the usability of end-user security software. In: Katsikas, S., Lopez, J., Soriano, M. (eds.) Trust, Privacy and Security in Digital Business. LNCS, vol. 6264, pp. 177–189. Springer, Heidelberg (2010)
17. Nurse, J., Creese, S., Goldsmith, M., Lamberts, K.: Guidelines for usable cybersecurity: past and present. In: Third International Workshop on Cyberspace Safety and Security (CSS), pp. 21–26. IEEE (2011)
18. Katsabas, D., Furnell, S., Downland, P.: Using human computer interaction principles to promote usable security. In: 5th International Network Conference (2005)
19. Bonastre, L., Granollers, T.: A set of heuristics for user experience evaluation in e-commerce websites. In: 7th International Conference on Advances in Computer-Human Interactions, IARIA, pp. 27–34 (2014)
20. Cranor, L., Garfinkel, S.: Security and Usability: Designing Secure Systems that People can Use. O'Reilly Media, California (2005)
21. Johnston, J., Eloff, J., Labuschagne, L.: Security and human computer interfaces. Comput. Secur. **22**, 675–684 (2003)
22. Nielsen, J., Molich, R.: Heuristic evaluation of user interfaces. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 249–256. ACM (1990)
23. Renaud, K.: Quantifying the quality of web authentication mechanisms a usability. Perspect. J. Web Eng. **3**, 95–123 (2003)
24. Braz, C., Seffah, A., Poirier, P.: Designing usable, yet secure user authentication services: a user authentication protocol. In: 5th International Conference on Applied Human Factors and Ergonomics, vol. 20, AHFE, pp. 155–165 (2014)
25. Fritsch, L., Fuglerud, K., Solheim, I.: Towards inclusive identity management. Identity Inf. Soc. **3**, 515–538 (2010)