Adding Measures to Task Models for Usability Inspection of the Cloud Access Control Services

Bilal Naqvi[1](✉), Ahmed Seffah[1], and Christina Braz[2]

[1] Lappeenranta University of Technology, LUT, Lappeenranta, Finland
Syed.naqvi@student.lut.fi
[2] Scotia Bank, Toronto, Canada

Abstract. Access control services in the cloud require defining which users, applications, or functions can have access to which data to perform what kinds of operations. There are thus three dimensions: (1) which users can (2) perform which operations (3) on which data. We speak of: (1) principals (i.e., users or roles), (2) privileges, and (3) objects, corresponding to these three dimensions, respectively. The act of accessing gives rights and privileges such as using or releasing data, modifying the access rights or accomplishing certain tasks. Permission to access also requires identity management. Research studies identify the existence of dependency between usability and security, and that there exists a conflict between the two, for which trade-offs are difficult to evaluate and engineer. This paper proposes a novel methodology for assessing the usability of access control services while ensuring that security requirements are met. The proposed methodology assists in integrating the experience of both security and usability experts by using different Human Computer Interaction methods as a way to identify the usability and security problems in access control security services in the cloud, and capture solutions to resolve such problems.

Keywords: Usable security
Usability in cloud access control and identity management
Usability of security services, security and usability conflict

1 Introduction

In recent years, there has been a significant growth in the adoption and popularity of the cloud-computing segment. However, such growth poses numerous challenges regarding security, usability, environmental sustainability etc. [13]. A wide range of users using different access devices, procedures, and technologies use cloud systems and security services. In cloud computing, authentication is a core requirement and serious concern as access control services protect not only critical IT infrastructures, but also related physical spaces including surveillance rooms, data centers, etc. Access control services in the cloud require defining which users, applications, or functions can have access to which data to perform which kinds of operations. The security challenge concerning user authentication and identity management services includes: (1) authentication, the process of verifying that an individual truly is who s/he claims to be

Published by Springer Nature Switzerland AG 2019
C. Bogdan et al. (Eds.): HCSE 2018, LNCS 11262, pp. 133–145, 2019.
https://doi.org/10.1007/978-3-030-05909-5_8

and (2) authorization, the process of assigning permissions to users [17]. There are thus three dimensions: (1) which users can (2) perform which operations (3) on which data. Corresponding to these three dimensions, we speak of: (1) principals (i.e., users or roles), (2) privileges, and (3) objects, respectively.

According to Cranor et al. [5], Jøsang et al. [11] and Nielsen [15], security and usability are considered as two opposed quality characteristics related to the user interface and functionality of the security system. One observable belief is that usability advocates support making it easy to use a system, preferably requiring no special access procedures at all, whereas security experts' support making it hard to access a system, at least for unauthorized users. However, there are several cases in which security and usability should be enhanced by modeling their mutual relationships, as an example of such cases, online payment, and e-banking, supervision of critical industrial infrastructures, crisis management and rescue systems. Therefore, more attention should be paid to the front-end of these secure solutions, i.e., how security information is communicated directly and indirectly to users. Usability cannot be treated separately from the security engineering of a system.

This research is a part of a long term project, where the main goal is to propose a framework for assessing the security and usability conflicts in access control services in the cloud while incorporating software measures into HCI task modeling techniques.

2 Measures of Usability in HCI and Security in Software Engineering

Security and usability have been widely recognized as two opposed characteristics [11]. Such opposed relation can be attributed for different reasons. The failure of security experts to measure usability is that usability problems with security systems and services are not just about the UIs usability. Existing literature highlighted that using conventional methods for usability evaluation only assess the usability impact on security effectiveness [12]. Usability and security conflicts and measures should be looked at from different levels. The ISO 27000 series of standards [10] identifies measurable attributes of information security as preservation of confidentiality, authenticity, accountability, non-repudiation, reliability, integrity and availability of information. Such attributes play an important role in measuring that the identified security requirements have been met.

Several researchers have introduced different methods to facilitate the development of usable secure systems. Kainda et al. [12] introduced a security usability threat model. They identified different usability and security factors based on previous studies and categorized them into six different groups of security topics. Authentication is one of these groups. However, the authors have not provided an example to clarify how the proposed model can be applied to measure the usability of security systems. Hausawi and Allen [7] proposed a summative usable security evaluation matrix that aims to help in determining the levels of usability and security quality attributes during the software development lifecycle; their matrix includes three usability factors (efficiency, effectiveness, and satisfaction) and three security factors (confidentiality, integrity, and availability). Zhao and Yue [20] introduced a Cloud-based Storage to manage browser-based passwords, their approach aimed to achieve a high level of security and usability with the desired confidentiality, integrity, and availability properties.

Hayashi et al. [9] introduced a usable security framework, called context-aware scalable authentication, which aims to use multiple implicit factors, such as a user's location, in order to select an appropriate active authentication form to authenticate the user. Nayak et al. [14] sought to enhance the security of the cloud services by introducing mutual authentication scheme using symmetric keys. During the authentication process, the proposed scheme requires the users to login into two accounts, indeed, that may make users feel uncomfortable. Beckerle and Martucci [2] introduced six guidelines for designing usable access control rule sets; they clarified that implementing those guidelines will help in understanding and managing access policies. Hausawi et al. [8] proposed an authentication system, called Choice-Based Authentication Approach (CBAA) which aims to provide better usability by allowing end users to select their authentication method based on their preferences. The authors pointed out that their approach improves security by increasing the difficulty for adversaries by displaying all of the possible authentication methods during the login process. Similar to the CBAA approach, Forget et al. [6] proposed an authentication architecture, called Choose Your Own Authentication (CYOA) which allows users to select a scheme amongst several available options. CYOA enables users to select whichever scheme best suits their preferences, abilities, and usage context.

Faily and Flechais [21], suggest using scenarios to describe how design decisions can lead to an unintentional security compromise caused by the end-user. They further present that these misusability cases can be used to impact design decisions of the developers and to bridge gaps between usability and security.

In the literature, various definitions concerning different attributes (facets, aspects, factors) of usability have been proposed. While security has been interpreted as a purely technical aspect in software development methodologies, some authors think it is more than that, taking instead a strategic dimension, resulting in one of the most important criteria in the governance of Information Communication Technology (ICT). For example, the executive management in companies still think that security technology is all that is required, and therefore 'delegates or downgrades' the issue to the technical departments, and conveniently neglects about the human and organizational concerns [19].

3 Proposal for Usable Security Measurement

The usability security measurement methodology (*see* Fig. 1) proposed in this paper was developed based on the original concept presented in Braz et al. [3], it aims to achieve this goal specifically while: (1) defining the possible conflicts between usability and security in terms of measures and (2) incorporating these measures into task models and a task-based inspection method. Task models are used to identify and model qualitatively the problematic aspects of the conflicts between usability and security. In comparison with Braz et al. work [5], we have used the ISO 25000 standard series and different measures as a way to quantify, assess and estimate quantitatively how security and usability are connected and how much severe the problem.

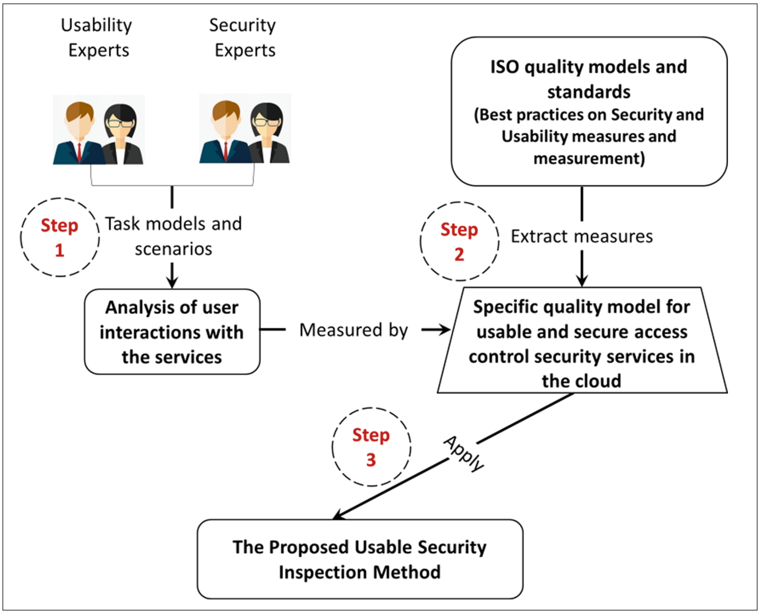

Usability Experts
Security Experts
ISO quality models and standards (Best practices on Security and Usability measures and measurement)
Step 1
Task models and scenarios
Step 2
Extract measures
Analysis of user interactions with the services
Measured by
Specific quality model for usable and secure access control security services in the cloud
Step 3
Apply
The Proposed Usable Security Inspection Method

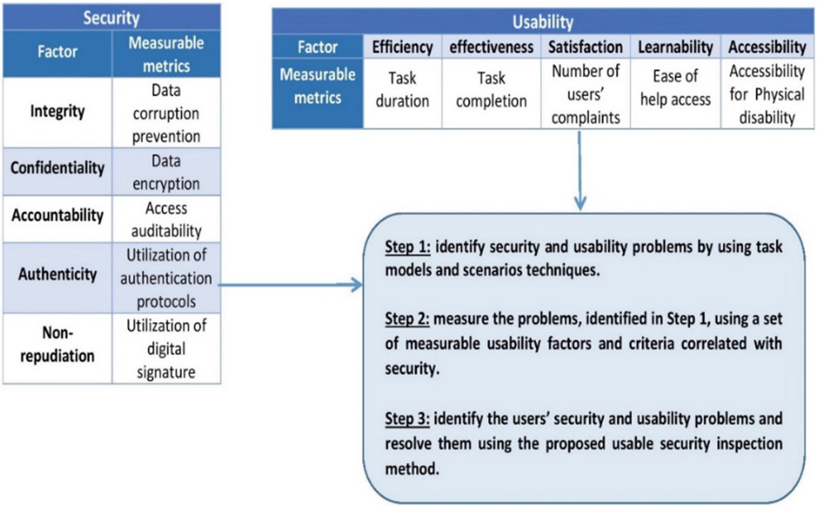
Fig. 1. The proposed usable security measurement methodology

The proposed usable security inspection method was developed using the design science research framework [16]. Following are the three steps of usable security measurement methodology that we propose.

- Step 1 describes how the task models and scenarios can be used by the usability specialists and security experts to analyze the users' interaction with the security services and then identifying and describing both the usability and security problems.
- Step 2 measures the usability and security interdependencies for each task model and the related security and usability problems using a set of measurable usability factors and criteria, correlated with security.
- Step 3 describes how the usable security inspection method is used to assist both the usability and security evaluators in identifying and evaluating the usability of security services. As detailed later, the method will help in the identification of the security and usability users' problems and their severity rate, with respect to the usability criteria and security measures defined in Step 2.

Figure 2 portrays a subset of these measures. For example, the authenticity factor can be measured using the authentication protocols.

$$UAP = X/Y$$



Security	
Factor	Measurable metrics
Integrity	Data corruption prevention
Confidentiality	Data encryption
Accountability	Access auditability
Authenticity	Utilization of authentication protocols
Non-repudiation	Utilization of digital signature

Usability					
Factor	Efficiency	effectiveness	Satisfaction	Learnability	Accessibility
Measurable metrics	Task duration	Task completion	Number of users' complaints	Ease of help access	Accessibility for Physical disability

Step 1: identify security and usability problems by using task models and scenarios techniques.

Step 2: measure the problems, identified in Step 1, using a set of measurable usability factors and criteria correlated with security.

Step 3: identify the users' security and usability problems and resolve them using the proposed usable security inspection method.

Fig. 2. A possible conflict between authenticity and satisfaction measures

Where UAP stands for utilization of authentication protocols, X is the number of provided authentication protocols, and Y is the number of required authentication protocols that are stated in the requirement specifications. In the same way, usability can be assessed using the satisfaction factor that can be measured using the number of user complaints

$$NUC = A/B$$

Where NUC stands for number of user complaints, A is the number of users' complaints and B is the total number of users. These two ratios help in determining to which extent the usability and security separately can be quantified [1]. Figure 2 shows a possible conflict between authenticity and satisfaction measures. Based on the first step of the proposed methodology, the users' interaction should be analyzed to identify the security and usability problems qualitatively.

For example, a multipurpose contactless smart card token-based authentication (i.e., PIN) is selected to authenticate a user to access to a Multifunction Teller Machine (Table 1). This protocol may affect the users' satisfaction negatively. Security and usability experts can use the task models and scenarios techniques to identify both security and usability problems that lead to the user non-satisfaction for example, consider the task and scenario below.

Task: *Authenticate user to a Multifunction Teller Machine (MTM)*
Scenario: User must authenticate her/himself through a multipurpose contactless smart card token-based authentication (i.e., PIN) in order to have access to different systems.

Table 1. Related problems from both the usability and security perspectives for the considered task

Usability	Security
Problem: Minimal Action (User Convenience: dealing with multipurpose VS. single purpose smart cards). Perspective: - The card improves user convenience since the user doesn't need to carry several cards and memorizing different PIN codes. However, it raises the risk that if the card is lost or gets stolen. - Using a one purpose card is more secure, but this means the user will need to carry one card for each application which is not as convenient.	Problem: Storage of Information. Perspective: - A multipurpose contactless smart card puts more sensitive information on the card - The risk involved when the wrong person gets access to the card, is much higher. - Contactless smart cards open the door to attacks that exploit over-the-air communication channels in an unsolicited way such as eavesdropping, interruption of operations, covert transactions, and denial of service.

Step 1: Identifying the Task Modeling and Scenarios

We used scenarios and tasks models, two well-known HCI techniques for analyzing users and usability problems as well as for understanding and modeling users' characteristics and the context in which the security and usability conflicts occurs.

We introduced a novel definition for a security and usability scenario as follows: a security scenario can be tangible or intangible. A Tangible Security Scenario (TSS) includes physical infrastructure such as control of user's access to buildings and facilities using: for example, biometrics, sending a silent alarm in response to a threat at a Multi-function Teller Machine (MTM), a type of an advanced ATM which provides additional services alongside cash withdrawal, such as video surveillance. An Intangible Security Scenario (ISS) includes data or other digital information: for example, a user who enters sensitive information at registration in order to purchase a concert ticket at an MTM. Both security and usability scenarios aim to detect the security and usability problems that may result when performing a task in a specific context.

To model the tasks and related scenarios, the GOMS (Goals, Operators, Methods, and Selection rules), a family of HCI techniques [4] has been used. GOMS helps the HCI analyst and security designer in making design decisions regarding the required tradeoff between usability and security when they come into conflict. For example, instead of determining and describing the recall password process within an existing Risk-based authentication method, the analyst-designer describes and decides how this user will use such process. Our choice of GOMS was mainly due to our knowledge and previous practical experience of using GOMS method for modelling task and scenarios.

Step 2: Connecting the Tasks' Scenarios with the Related Usability Criteria and Factors

Here, we model security as a usability sub-characteristic: both usability and security are defined in terms of sub-factors that are measures. Seffah et al. [18] introduced a Quality in Use Integrated Measurement (QUIM) model as a consolidated model for measuring usability. As part of our proposed methodology, we selected nine usability sub-factors from the QUIM model, where the selected factors are related with security. The selected usability factors namely efficiency, satisfaction, productivity etc. are presented in Fig. 3.

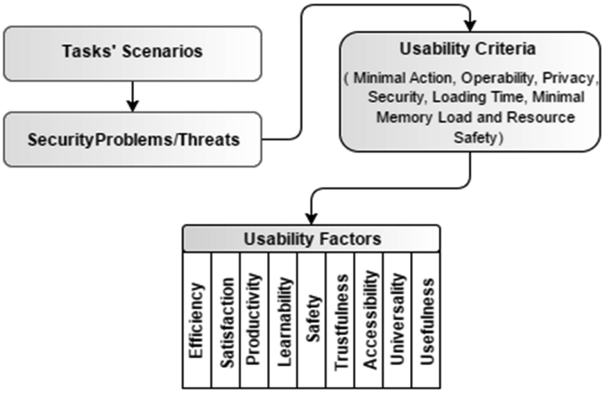


Fig. 3. Connecting the tasks' scenarios and their security problems with the corresponding usability criteria and factors

Each of these factors is broken down into one of the following measurable criteria:

- *Minimal Action* (capability of the application to help users achieve their tasks in a minimum number of steps);
- *Minimal Memory Load* (whether a user is required to keep minimal amount of information in mind in order to achieve a specified task);
- *Operability* (amount of effort necessary to operate and control an application);
- *Privacy* (whether users' personal information is appropriately protected);
- *Security* (capability of the application to protect information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access);
- *Load Time* (time required for the application to load (i.e., how fast it responds to the user);
- *Resource Safety* (whether resources including people are handled properly without any hazard).

Therefore, after identifying the tasks' scenarios, security experts should analyze them and identify the security problems or threats that may result from each scenario. Thereafter, both usability and security experts should analyze these problems, in order to identify the corresponding usability criteria. Finally, the usability criteria should be mapped to one or more measurable usability factors. In fact, the relation between usability criteria, factors, and security problems can be used to guide a design decision or to assess a design that has already been created.

Step 3: Applying Usability Security Inspection Method
In HCI, inspection is a set of techniques which consist of evaluators to examine, for example, computer security software without involving end users. The method can be used in conjunction with task modeling and with modeling of security as usability sub-factor. Inspection can be conducted during the early phases, mainly requirements analysis and preliminary design phases that help security designers to identify possible problems as early as possible.

As part of our methodology, we developed a heuristic-based method, called usable security inspection. It involves having a group of evaluators, mainly security and HCI designers, to systematically examine the user interface of a security protocol (e.g. authentication) and judge its compliance with security and usability principles. The interface is regarded, in this paper, as both software (e.g. user logs into a Website) and hardware components (e.g. authentication token) towards which the interaction and information transit between software and/or hardware components, network, and users.

The output of this inspection method is a checklist that aims to evaluate the authentication method that will be used to authenticate users. After generating the inspection method checklist, the security and usability evaluators will be able to identify security and usability problems and their severity rates. However, users' usability and security problems are rated by three severity levels:

- *Major*: refers to catastrophic problems that should be given a high fixing priority level, they must be fixed before releasing the software.
- *Intermediate:* it is important to fix this type of problem as soon as possible.
- *Minor*: refers to problems with a low fixing priority level, which means that these problems should be fixed only if there is extra time available.

4 Case Study

This section aims to clarify how to use the proposed usable security measurement methodology for developing usable and secure authentication method to access Multifunction Teller Machine (MTM) account through the user phone.

Step 1: Identifying the MTM's Task Models and Scenarios
The users' tasks to use MTM may include: authenticate user to a system, transfer funds to an international bank account, buy a ticket concert, access a MTM through a mobile phone, deposit a check using checking image and send a silent alarm. For example Table 2 clarifies the related scenario and the required features for the task below.

Task: *Access and authenticate to MTM with your mobile phone*

Based on this scenario, we have identified the usability and security problems and their related perspectives (see Table 3).

Table 2. An example task to access MTM with mobile phone, its related scenario and sub-tasks

Scenario	Sub-Tasks
Customer accesses a MTM via mobile phone in order to make his/her mortgage monthly payment. The phone is equipped with a special chip that enables to communicate with the MTM	Sub-tasks performed using a mobile phone: 1. Select "Access my MTM" from the cell phone main menu; 2. Enter your 4 digit PIN (the PIN is entered on the customer's phone keypad then transmitted to a central server and checked against file saved there); 3. Select "Make a Payment" from the MTM's menu; 4. Select the type of payment which is "Mortgage"; 5. Tap the exact amount; 6. Select "Submit".

Table 3. Usability and security problems associated with the considered task

Usability	Security
Problem: Overwhelm Customers with complexity when dealing with different communication channels.	**Problem:** Credentials across several channels
Perspective - Customers have to manage complexity when dealing with different services offered through different types of communication channels such as MTM, Web, and WAP. - Customers will still be required to authenticate to the system by entering a PIN. Unlike passwords, PINs have no meaning to the customer, and then it might be even harder to remember than a password (i.e., passwords can be created to be pronounceable). PINs become harder to remember for customers who have many different ones to keep track of.	**Perspective** - Using the same authentication credentials for both WAP and MTM channel, can provide convenience for the customers. However, PIN code is the only acceptable alternative for the WAP channel, and is not considered to provide good enough security (i.e., longer PINs (6 or 8 digit PINs) would be more secure than 4-digit PINs). - Additionally, when PIN is used for authentication over the phone, the risk of eavesdropping the telephone line is a supplementary threat, especially since it cannot be encrypted.

Step 2: Connecting the Tasks' Scenarios with the Related Usability Criteria and Factors

Let us consider the task scenario detailed in the previous step to illustrate the applicability of the usability factors and their corresponding criteria using MTM tasks. Table 4 illustrates the procedure to adopt for connecting the tasks scenarios to the related usability criteria and factors.

In addition, for measurement purpose QUIM suggested 127 measures for usability factors [18]. However, other measures can be used for measuring such factors, such as

Table 4. Mapping the tasks' scenarios to the nine usability factors and eight usability criteria

Task Scenario	Security Problem/Threat	Measurable Usability Criterion	USABILITY FACTORS								
			Efficiency	Satisfaction	Productivity	Learnability	Safety	Trustfulness	Accessibility	Universality	Usefulness
Authenticate user to a system	– Storage of Information – Replay attacks – Eavesdropping – Session hijacking – Man-in-the-middle – Verifier impersonation.	**Minimal Action**	●	●		●			●		

those proposed in ISO 25022 [10]. For example, the efficiency can be measured, by measuring how cost-effective is the user, using the following formula:

$$X = TE/C$$

Where TE is the task effectiveness, which refers to whether the task is executed correctly or not, and C is the total cost of the task, where costs could, for example, include the user's time, the time of others giving assistance, and the cost of computing resources.

Step 3: Applying the Usability Security Inspection Method
Based on discussion in Sect. 3 (step 3), we have identified examples of the security and usability review questions in order to generate the usability security inspection method checklist (see Table 5).

From the generated checklist, we have identified security problems, their severity rates and recommendations to resolve them (see Table 6).

Table 5. An example of the usable security inspection method checklist

Usable Security Inspection Method										
Usability Criteria: Security										
Description: Capability of the application to protect information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access										
#	**Usability Review**	**Occurrence**			**Comments**	**Security Review**	**Occurrence**			**Comments**
1.1	When using different communication channels, is PIN authentication used (i.e., when accessing MTM, Web, and WAP: PINs are easier to remember)?	Y	N	Y / N	-----	Is 6-digits PIN used (i.e. PINs have lower level of security since the number of possible combinations is lower[1])?	Y	N	Y / N	It needs system review to be able to implement it.
		🟩						🟥		
[1] Long PINs give stronger security, but bad usability because the PIN is harder to remember and takes longer to type. [2] With enough memory and/or a crypto processor [3] This would provide a higher level of security but lower system response time and thereby usability. The risk of eavesdropping the telephone network is a real threat, especially since it cannot be encrypted.										

Table 6. An example of security problems related to the security usability criteria

Problem description	Usability criteria	Severity rate	Security Issue	Interdependencies	Recommendations
Unsafe PIN length (Security review1.1)	Security	Major	A MTM machine relies on short, low-entropy PINs for authentication. A four-digit PIN can be broken in less than a second, and a 6-digit PIN in about 10 s, while a 10-digit PIN would likely take weeks to crack.	Performance, efficiency.	(ISO 9564-1 :2002) allows for PINs from 4 up to 12 digits, but also notes that for usability reasons, an assigned numeric PIN should not exceed six digits in length. So ideally, use PINs with a large number of digits for instance a 6-digit PIN.

5 Conclusion

This paper presents a methodological approach for measuring usable security conflicts while featuring how to supplement tasks models with measures for access control services in the cloud. A practical contribution is the use of such approach for the evaluation of access control security services in the context of cloud. The enhanced task models with measures aimed at detailing the interrelationships and conflicts between security and usability. In comparison with the existing models for designing usable security authentication mechanisms (such as [15]), the approach introduces clear steps to improve the usability of user authentication and access control services in the cloud. An important aspect is that the methodology does not only point out general security and usability recommendations, but specifies explicitly how a compromise can be established when these two key factors come into conflict.

References

1. Azuma, M.: Software products evaluation system: quality models, metrics and processes—International Standards and Japanese practice. Inf. Softw. Technol. **38**(3), 145–154 (1996)
2. Beckerle, M., Martucci, L.A.: Formal definitions for usable access control rule sets from goals to metrics. In: Proceedings of the Ninth Symposium on Usable Privacy and Security. ACM (2013)
3. Braz, C., Seffah, A., Naqvi, B.: Integrating a Usable Security Protocol into User Authentication Services Design Process. CRC Press, Boca Raton (2018)
4. Card, S.K., Newell, A., Moran, T.P.: The psychology of human-computer interaction (1983)
5. Cranor, L.F., Garfinkel, S.: Security and Usability: Designing Secure Systems that People Can Use. O'Reilly Media Inc., Farnham (2005)
6. Forget, A., Chiasson, S., Biddle, R.: Choose your own authentication. In: Proceedings of the 2015 New Security Paradigms Workshop, pp. 1–15. ACM (2015)
7. Hausawi, Y.M., Allen, W.H.: Usable-security evaluation. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2015. LNCS, vol. 9190, pp. 335–346. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-20376-8_30
8. Hausawi, Y.M., Allen, W.H., Bahr, G.S.: Choice-based authentication: a usable-security approach. In: Stephanidis, C., Antona, M. (eds.) UAHCI 2014. LNCS, vol. 8513, pp. 114–124. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07437-5_12
9. Hayashi, E., Das, S., Amini, S., Hong, J., Oakley, I.: CASA: context-aware scalable authentication. In: Proceedings of the Ninth Symposium on Usable Privacy and Security. ACM (2013)
10. ISO/IEC: ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary. International Organization for Standardization (2014)
11. Jøsang, A., Zomai, M.A., Suriadi, S.: Usability and privacy in identity management architectures. In: Proceedings of the Fifth Australasian Symposium on ACSW Frontiers, vol. 68, pp. 143–152. Australian Computer Society, Inc. (2007)
12. Kainda, R., Flechais, I., Roscoe, A.: Security and usability: analysis and evaluation. In: International Conference on Availability, Reliability, and Security, ARES 2010, pp. 275–282. IEEE (2010)

13. Marinos, A., Briscoe, G.: Community cloud computing. In: Jaatun, M.G., Zhao, G., Rong, C. (eds.) CloudCom 2009. LNCS, vol. 5931, pp. 472–484. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10665-1_43
14. Nayak, S.K., Mohapatra, S., Majhi, B.: An improved mutual authentication framework for cloud computing. Int. J. Comput. Appl. **52**, 5 (2012)
15. Nielsen, J.: Security & Human Factors (2000). https://www.nngroup.com/articles/security-and-human-factors/
16. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A design science research methodology for information systems research. J. Manag. Inf. Syst. **24**(3), 45–77 (2007)
17. Salini, P., Kanmani, S.: Survey and analysis on security requirements engineering. Comput. Electr. Eng. **38**(6), 1785–1797 (2012)
18. Seffah, A., Donyaee, M., Kline, R.B., Padda, H.K.: Usability measurement and metrics: a consolidated model. Softw. Qual. J. **14**(2), 159–178 (2006)
19. Von Solms, B., Von Solms, R.: The 10 deadly sins of information security management. Comput. Secur. **23**(5), 371–376 (2004)
20. Zhao, R., Yue, C.: Toward a secure and usable cloud-based password manager for web browsers. Comput. Secur. **46**(10), 32–47 (2014)
21. Faily, S., Fléchais, I.: Finding and resolving security mis-usability with mis-usability cases. Requirement Eng. **21**(2), 209–223 (2016)