Interdependencies, Conflicts and Trade-Offs Between Security and Usability: Why and How Should We Engineer Them?

Bilal Naqvi[1,2] and Ahmed Seffah[3]

[1] Software Engineering, LENS, LUT University, Lappeenranta, Finland
syed.naqvi@student.lut.fi
[2] Mirpur University of Science and Technology, MUST, Mirpur, Pakistan
[3] Green UX Design, Thinking Associates, Paris, France

Abstract. Security and usability are considered as conflicting goals. Despite the recognition that security and usability conflicts pose a serious challenge to achieve effective security, the review of the state of art identifies many gaps in today's practices including, (1) failure of security specialists to address usability, as perceived and defined by the human computer interaction (HCI) community, (2) industry's behavior is being more driven by bug fixing, rather than trying to examine and consider the context and the human experiences in which the bugs occurs, and (3) the lack of HCI skills required for conducting effective user studies. Furthermore, analysis of the existing literature identifies different perceptions concerning the relationship between security and usability. Some researchers have identified existence of trade-offs when it comes to the security and usability conflicts, however, others refer to the trade-offs as mere myths. A four staged process oriented framework to address the security and usability conflict is presented in this paper. The framework governs aspects from identification of the conflicts to elicitation of suitable trade-offs. To support re-use, the outcomes of employing the framework are documented in form of design patterns. A template to standardize documentation of the patterns is also presented along with one example of the usable security patterns.

Keywords: Usability · Security · Usable security · Conflicts · Trade-offs · Framework · Patterns · Usable security patterns

1 Introduction

ISO 25010 model lists security and usability among the eight characteristics of its product quality model [1]. Despite providing guidance on handling each quality characteristic individually, ISO 25010 does not provide guidance when two or more dependent characteristics come into conflict. An example of such a conflict is the conflict between security and usability. As an instance of security and usability conflict consider passwords; despite their role in implementing authentication (a security mechanism), passwords have a human dimension. The password security guidelines suggest passwords to be sufficiently long, frequently changed, have different cases and special characters, etc., however, from user's perspective such passwords are hard to

A. Moallem (Ed.): HCII 2019, LNCS 11594, pp. 314–324, 2019.
https://doi.org/10.1007/978-3-030-22351-9_21

memorize especially when re-use of the passwords is strongly discouraged and an average user has to manage around 22 online password [2].

Password masking is another instance of the security and usability conflict. To protect against shoulder surfing and other similar attacks, almost all authentication implementations mask the password when the user types it. However, for a legitimate user it impacts usability element of 'feedback' as in case of a mistake the user has to re-type long complex password, rather than knowing and correcting the mistake. Therefore, it can be gathered that password masking approach holds good from security perspective, but it has an impact from the usability point of view.

Human factors are perhaps considered as greatest barrier to effective computer security [3]. Most security mechanisms are too difficult and confusing for the average computer user to manage correctly. Furthermore, a common belief is that security and usability are two the opposed quality factors that are related to different components of a system (functionality and user interface respectively). This means that, security of the system and usability of the services can be engineered by two separate teams, mainly by software engineering and user interface (UI)/user experience (UX) teams. However, there are several cases in which security and usability are enhanced by modelling their mutual relationships. Typical examples include online payment and e-banking services, supervision of critical industrial infrastructures, crisis management. This research aims to bridge the gaps between security specialists and UI/UX experts. The following are the key gaps:

One gap explains the failure of security specialists to address usability, as perceived and defined by the HCI community. Security and usability have historically evolved independently or have been considered as two opposite factors. Another historical explanation is that researchers were more driven by technology rather than user problems and perceptions of security. For example, the development of identity management technologies was so demanding in terms of security that it left little time and costs to cater usability and the human factors in general.

A second gap that may be advocated is the industry's behaviors is more driven by bug fixing, rather than trying to examine and consider the context and the user experiences in which the bugs occurs. Therefore, most industry efforts have been on automating the process of reporting and handling bugs, rather than looking for human experiences and how they can promote more secure operations overall.

Another gap that demonstrates the lack of alignment between security and usability is the design and innovation approach leading to new security technologies. Most often, the innovation is initiated by a company developing an "in-house technology" addressing a specific problem which occurs in a specific project. Other groups in the same company or others companies may develop their own versions of these solutions. This makes it difficult to ensure the usability of these in-house solutions and several versions of them, while changing the original context of their applicability. Fire-walls, junk mail filters, spyware, and antivirus are good examples.

Finally, the lack of HCI skills required for conducting effective user studies are a serious obstacle. Moreover, user studies are difficult to conduct because regulations governing use of human subjects' in experiments related to safety and security of the systems and services have to be considered.

Despite these gaps and non-alignment between security and usability, the conflict between these two is a recognized problem; the primary question addressed in this paper is why and how to engineer the conflicts and trade-offs between security and usability. One approach that we consider appropriate for engineering the conflicts and appropriate trade-offs involves the use of design patterns. Patterns can be used to document instances of the conflict and balanced solution to address the conflict (right trade-off). Patterns can be disseminated among the community of security and usability developers to influence their decision making when it comes to the conflict between the two characteristics.

The remainder of this paper is organized as follows. Section 2 presents the literature review, which was conducted considering two main objectives. Section 3 discusses the primary question addressed in the paper i.e. why and how to engineer the conflicts and trade-offs between security and usability, both 'why' and 'how' to engineer conflicts and trade-offs are discussed in subsequent sub-sections. A template to standardize documentation of the patterns is also presented along with one example of the usable security patterns. Section 4 concludes the paper.

2 Literature Review

Despite the recognition of security and usability conflict as a challenge, not much has been accomplished for two reasons, (1) security and usability are considered as after thoughts, and (2) security and usability are not considered strategically, and not integrated into to the strategic plans for system development [4].

The literature review was conducted in two stages with objectives as follows.

1. To identify one of the core reasons for non-alignment between security and usability.
2. To identify solutions for addressing security and usability conflicts.

The result of the first stage of literature review revealed inconsistent perceptions about relationship between security and usability as one of the reasons for non-alignment between the two characteristics. However, the findings relevant to both objectives are presented in subsequent sub-sections.

2.1 Inconsistent Perceptions About Relationship Between Security and Usability

Various communities and interest groups have been studying the security and usability conflicts independently from each other, these include: (1) traditional computer security community dealing with the wider scope of quality of services in computer and communication technologies; usability is a minor concern addressed at a cosmetic level in this community, (2) the software engineering community where security and usability have been defined as two among the eight major quality characteristics, and usability is a characteristic of user interfaces and security is a characteristic of the functionality, (3) the HCI community, to name a few. As a result, the available literature on relationships between security and usability can be classified in two categories.

- There are trade-offs when it comes to conflicts between security and usability.
- Trade-offs between security and usability are mere myths.

Most of the research till date argues on existence of the trade-offs between security and usability. The authors [5] conducted a case study on iOS and Android to find an answer for “what is more important: usability or security”. The authors identified that importance of security and usability is purely situation based, and that the trade-offs are sometimes in favor of security and vice versa. The authors [6] presented an empirical evidence in favor of existence of the trade-offs between security and usability. The empirical study featured three different schemes for code voting systems. The authors state, “nevertheless, the security gains come at the cost of usability losses”. The authors [7] presented an empirical investigation concerning existence of trade-offs between security and usability. The results of within-subjects study to understand and value security and usability trade-offs in end-to-end email encryption were presented. The results of the study identify that the participants in their choice for the preferred system to use deliberately made the trade-offs between security and usability.

In parallel with the research establishing existence of the trade-offs, there is some research classifying security and usability trade-offs as mere myths. A special issue ‘the security-usability trade-off myth’ features one such discussion between researchers and practitioners in usable security [8]. The participants were of the view that decreasing usability can lead to less security and understanding the context in which solutions are deployed is important. The participants discussed the example of two-factor authentication involving one-time passwords (OTP) and its consequences if the length of OTP is increased from 6 to 8 characters. Overall, the participants were of the view that, “security experts simply invoke the myth of tradeoff between usability and security, and use this as cover to avoid the exercise of saying precisely what security benefit in precisely what scenarios this usability burden is going to deliver.” The authors [9] stated that security and usability are not inherently in conflict. The authors suggested that the researchers have to go beyond than just adopting human-centered design principles and consider involving the user in the decision making process.

2.2 Solutions to Address the Security and Usability Conflicts

In line with the second objective of the literature review, we present the solutions that have been proposed to address the security and usability conflict. The author [10] presented a set of guidelines to cater the security and usability conflict. The work is mainly focused on avoiding the conflict by depriving the user from making system security related decisions. The author presented guidelines like, providing a check-list to developers of security systems, hiding security related tasks from users, reducing the user memory load etc. The author also suggested that user should be involved in making security decisions on the system only when the situation is clear to the user; otherwise, the system should take the security decisions itself.

The authors [11] while studying the trade-offs between security and usability presented a set of guidelines to cater the conflict. The authors considered various aspects of usability such as effectiveness, satisfaction, efficiency, learnability and presented different guidelines focusing on each of the mentioned elements in conjunction with security.

The authors [12] suggested to implement security features as a separate service on cloud naming it CaaS "Confidentiality as a Service", which would perform the confidentiality function on behalf of the users even if the credentials are lost. The main theme discussed in their work is to create a level of abstraction, and let the service perform security tasks on user's behalf.

The authors [13] presented an ontological framework for catering the security and usability conflict. The framework is based on identification of usability/security requirements, identifying meaning and system context. After that the conflicts are identified on basis on system requirements, which are characterized on basis of their impact and listed. The nature of the identified conflict is then determined, and based on that the conflict resolution strategy is made in accordance with the system requirements.

The authors [14] presented an 'Assessment Framework for Usable Security' (AFUS), which works by filtering and merging the security and usability requirements, and then applying utility functions for risk analysis. The decision trees are generated to calculate the weight and utility of each attribute of security and usability. The weights determine relative importance of attributes to be considered for requirement specification of software. The authors claim that requirements specified after AFUS have a balance between usability, security and usable security.

3 Interdependencies, Conflicts and Tradeoffs Between Security and Usability: Why and How Should We Engineer Them?

3.1 Why Is It Important to Handle Security and Usability Conflicts?

Security cannot be achieved in real sense unless it incorporates the human element [22]. To establish why it is important to handle security and usability conflicts, we refer to some existing empirical evidences and technical reports. National Institute of Standards and Technology (NIST) report NISTIR 8080 states that "the human element is a critical yet often overlooked component during technology integration […], it is critical to understand users' primary goals, the characteristics of the users (both physical and cognitive attributes), and the context in which they are operating" [15].

IBM global analysis report on 'cost of data breach' mentions that a data breach caused by human error takes around 162 days to identify and 59 days to contain. Among the root causes of data breaches, the report identifies that 25% of data breaches are caused due to human factors [16]. Considering these stats in conjunction with NIST report, identifies one possible reason for such high number of breaches due to human errors i.e. due to overlooking human factors while designing the security systems. We extend this argument to postulate that security features are unnecessarily complex thereby increasing the chances of error.

As early as in 1998, Whitten and Tygar suggested the need for developers (of security functionality) to think from user's perspective. They further stated that designers of security systems should not assume that the users will read manuals for configuration, instead, the security should be easy to use [17].

The study [18] revealed results of analysis of 32 million passwords for a service, among which 1% were merely “123456” and around 20% of the passwords were the user’s name, slang or a common dictionary word. These stats basically describe the user’s will, as stated by authors [19], “unless you stand over them with a loaded gun, users will disable, evade, or avoid any security system that proves to be too burdensome or bothersome”.

Usable security poses a distinct challenge that needs to be addressed, while working on security of the system. With reference to stats discussed earlier, it is relevant to state that developing a system without incorporating human aspects even being secure against external threats, would be susceptible to: (1) user mistakes ultimately leading to system compromise, (2) increased user disengagement and frustration, (3) users working around anything necessary to do their job [20].

It is important to mention that security and usability conflict is not limited to usability of the interface, and should not also be considered as limited to studies featuring passwords and other authentication mechanisms; however, there are other instances of this conflict beyond just authentication and user interfaces. One such example features conflicts arising with deployment of complex encryption ciphers, which impact ‘understandability’ of human users while implementing ‘confidentiality’ (a security mechanism). Furthermore, the authors [20] state, “researchers have identified an increasing number of security mechanisms that are so unusable that the intended users either circumvent them or give up on a service rather than suffer the security”. Therefore, it is imperative to consider all aspects of the conflict between security and usability, otherwise we risk building complex secure systems that are susceptible to user mistakes ultimately leading to security compromises.

3.2 How to Engineer the Security and Usability Conflicts?

Figure 1 portrays the proposed four-staged process oriented framework. The framework provides sequence of activities to be followed in order to address the conflict. The framework helps in identifying the conflicts between security and usability while documenting balanced solutions (right trade-offs) in the format of patterns. The four major activities that form basis of this framework are as under.

1. *Analysis* of the diverse human experiences and tasks of the stakeholders and end-users that involve security technologies, modeling of the interaction between stakeholders and user’s interaction to accomplish those tasks, and quantifying the possible usability problems.
2. *Modelling* of the relationship between security and usability using as input the descriptions of human experiences, tasks and usability problems identified in the previous step.
3. *Development* of the solutions and their documentation in the format of patterns. The solutions can be used by participating organizations to enhance usability of existing security technologies or the development of new ones.

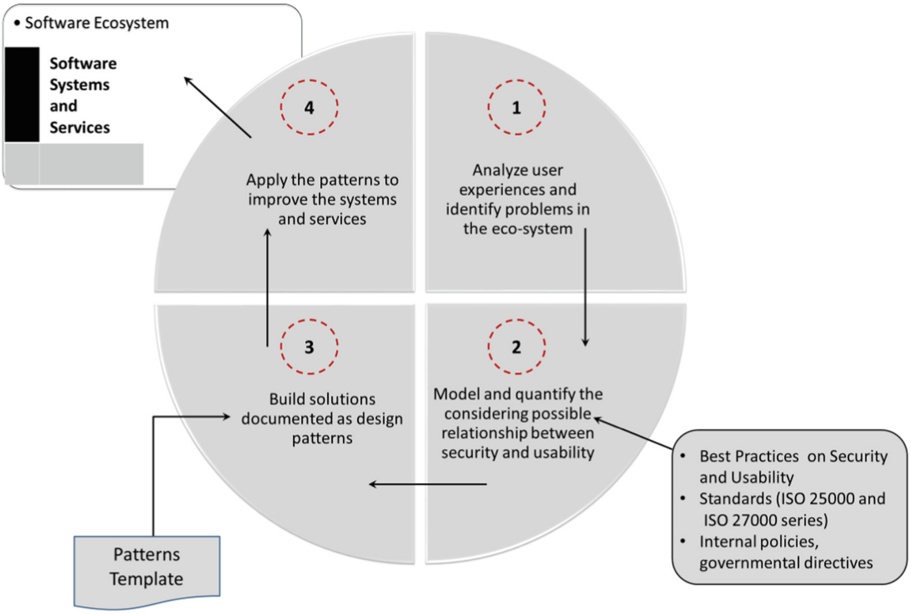
• Software Ecosystem
Software Systems and Services
4
Apply the patterns to improve the systems and services
1
Analyze user experiences and identify problems in the eco-system
3
Build solutions documented as design patterns
2
Model and quantify the considering possible relationship between security and usability
• Best Practices on Security and Usability
• Standards (ISO 25000 and ISO 27000 series)
• Internal policies, governmental directives
Patterns Template

Fig. 1. The proposed process-oriented framework for engineering conflicts between security and usability

4. *Application* of the documented patterns in the software eco-system. Pattern can serve as an effective tool for developers in order to deal with usability concerns in security services. Particularly, the patterns can serve less experienced developers and free-lancers in influencing their decision making abilities when it comes to the security and usability conflicts.

We have been developing and refining this framework using a series of experiments in lab and industry following a design science research (DSR) approach. The main advantage of DSR is the "build-and-evaluate" loop, which allows suggestions from community to be incorporated in the evolved versions of the framework.

As evident from the Fig. 1, the first step involves identification of the conflicts. For this purpose, user studies, cognitive walkthroughs, heuristic evaluations are conducted. Once the conflicts are identified the relationship between security and usability are modelled and quantified. Best practices and standards on security and usability also come into play when modelling the relationship between the two. When do's and don'ts from the perspective of security and usability are known after accessing the underlying best practices, standards and directives, the security and usability professionals brainstorm together to build a balanced solution (the right trade-off) between the two conflicting characteristics. The right trade-offs along with other necessary information are then documented as design patterns. A standardized template for documenting the usable security patterns is presented in Fig. 2.

Once the pattern is documented it can be applied to solve the recurring problem in the software eco-system in similar context of use. The pattern is expected to facilitate

- **Title:** The unique name of name for the pattern. Pattern can be named on basis of the problem it is solving or some names can be attributed to the solution suggested in the pattern.
- **Classification:** What is the category of the pattern, example categories can be: authentication mechanisms, data protection, device protection etc. Classifying patterns and grouping them would assist developers to find them under the relevant category.
- **Prologue:** One sentence that describes the intent behind this pattern.
- **Problem statement**: One or two sentences to summarize the problem addressed by the pattern.
- **Context of Use:** Patterns always have a particular context. A statement describing the context in which the particular patterns can be applied. The context should lack ambiguity so that the pattern is always applied in correct situations.
- **Affected Sub factors:** The sub-factors of usability and security being affected/involved when this pattern is applied.
    - Usability:
    - Security:
- **Solution:** One or two statements that guide on how to solve the problem.
- **Discussion:** Statements that illuminate the system of forces resolved (forces for us are the dimensions of conflicts) by the pattern.
- **Type of service**: Applicability of pattern from device/infrastructure perspective, e.g. mobile, desktop, web etc.
- **Epilogue:** One sentence per pattern that can be expected to follow this one or simply consequence of applying the pattern.
- **Related Patterns:** The patterns that are related to this pattern; this would provide information about similar patterns that can also be applicable whenever the problem (being addressed in this pattern) occurs.

Fig. 2. Usable security patterns template

developers and designers in making reasonably accurate choices when it comes to the conflicts between security and usability. Both usability and security professionals recognize the importance of incorporating their concerns throughout the design cycle and acknowledge the need for an iterative, rather than a linear design process. Design patterns have shown their effectiveness in supporting a smooth integration and cross-pollination of communities [21]. Patterns also assist in an improved communication among team members from different disciplines by developing a common language or vocabulary when explaining design. For elaborating how a usable security pattern would look like, an example pattern is presented in Fig. 3.

It is pertinent to state that one pattern solves one problem only, therefore, an entire catalogue of patterns is required to support the development of simultaneously usable and secure software systems. The documented patterns can be disseminated among the community of developers and designers using online pages, conducting developer workshops and symposiums, research publications, etc.

- **Title:** Visibility of system status.
- **Classification:** data protection, device protection.
- **Prologue:** To make the user feel satisfied after performing a security task.
- **Problem statement**: The completion of security task leaves the user wondering, if the task was completed to perfection or not.
- **Context of Use:** Whenever security task requires user intervention and user is able to complete the task to perfection. The 'security tasks' would include successful encryption and all other tasks relevant to data and device protection.
- **Affected Sub factors:** The sub-factors of usability and security being affected/involved when this pattern is applied.
    - Usability: trust, satisfaction, feedback
    - Security: confidentiality, integrity, non-repudiation
- **Solution:** In case of successful completion of a security task, provide the user with feedback followed by clear visibility of the system status. For example, when the communication has been encrypted change the window color that gives the user the protected feel.
- **Discussion:** Providing the user with clear feedback and visibility of status not only preserves system security, but increases the user trust and satisfaction towards the system.
- **Type of service**: mobile, desktop, web.
- **Epilogue:** Increased user satisfaction with no impact on security.
- **Related Patterns:** Can be added later from the catalogue.

Fig. 3. Visibility of system status pattern

4 Conclusion

Security cannot be achieved in real sense unless it is usable by the users. This research advocates an evolving approach from 'user is the problem' to 'user must be a part of technology based solution'. This paper research is an attempt towards aligning security and usability, and for that a process oriented framework is presented. The framework governs the process from identification of the conflicts to documentation of the right trade-offs in form of re-usable design patterns.

Design patterns can also prove to be effective in handling inconsistency of views between different communities, and between academia and industry, by providing shared documentation in form of patterns. The patterns' ability to be improved over the time provides a common ground to incorporate several views i.e. from industry and academia. With the use of patterns, it is imperative to ensure that they are applied in relevant context of use. We have also developed a usable security patterns template to standardize the documentation of the patterns. For standardized documentation, a pattern template encapsulating information like, title, classification, prologue, problem statement, context of use, solution, discussion, is presented in this paper. To instantiate the use of patterns, a novel pattern 'visibility of system status' is also presented. It is worthwhile to state that one pattern addresses only one instance of the conflict, therefore, it is unrealistic to expect a pattern to solve a systems' problem; however, a catalogue of patterns addressing different instances of the conflict between security and usability would be required in this regard.

References

1. ISO 25010, Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models (2011)
2. Password Guidance: Simplifying Your Approach. The National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach
3. Naqvi, B., Seffah, A.: A methodology for aligning usability and security in systems and services. In: International Conference on Information System Engineering (ICISE), pp. 61–66. IEEE (2018)
4. Dhillon, G., Oliveira, T., Susarapu, S., Caldeira, M.: Deciding between information security and usability: developing value based objectives. Comput. Hum. Behav. **61**, 656–666 (2016)
5. Garg, H., Choudhury, T., Kumar, P., Sabitha, S.: Comparison between significance of usability and security in HCI. In: 2017 3rd International Conference on Computational Intelligence Communication Technology (CICT), pp. 1–4 (2017)
6. Kulyk, O., Neumann, S., Budurushi, J., Volkamer, M.: Nothing comes for free: how much usability can you sacrifice for security? IEEE Secur. Priv. **15**, 24–29 (2017)
7. Bai, W., Kim, D., Namara, M., Qian, Y., Kelley, P.G., Mazurek, M.L.: Balancing security and usability in encrypted email. IEEE Internet Comput. **21**, 30–38 (2017)
8. Sasse, M.A., Smith, M., Herley, C., Lipford, H., Vaniea, K.: Debunking security–usability tradeo myths. IEEE Secur. Priv. **14**(5), 33–39 (2016)
9. Cranor, L.F., Buchler, N.: Better together: usability and security go hand in hand. IEEE Secur. Priv. **12**, 89–93 (2014)
10. Hof, H.-J.: User-centric IT security-how to design usable security mechanisms. In: 5th International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services (CENTRIC), pp. 7–12 (2012)
11. Sahar, F.: Tradeoffs between usability and security. Int. J. Eng. Tech. **5**, 434–437 (2013)
12. Fahl, S.: Confidentiality as a service—usable security for the cloud. In: 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 153–162 (2012)
13. Mairiza D., Zowghi, D.: An ontological framework to manage the relative conflicts between security and usability requirements. In: 3rd International Workshop on Managing Requirements Knowledge (MARK), pp. 1–6 (2010)
14. Hausawi, Y.M., Allen, W.H.: An assessment framework for usable-security based on decision science. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 33–44. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_4
15. National Institute of Standards and Technology. NISTIR 8080 Usability and Security Considerations for Public Safety Mobile Authentication (2016)
16. IBM: Cost of Data Breach Study: Global Analysis by Ponemon Institute LLC, Sponsored by IBM (2016)
17. Whitten, A., Tygar, J.D.: Usability of security: A case study. School of Computing Science, Carnegie Mellon University. Rep. Technical Report CMU-CS-98-155 (1998)
18. Imperva: Application Defense Center: Consumer Password Worst Practices. http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

19. Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., Möller, S.: On the need for different security methods on mobile phones. In: Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, pp. 465–473 (2011)
20. Glass, B.D., Jenkinson, G., Liu, Y., Sasse, M.A., Stajano, F., Spencer, M.: The usability canary in the security coal mine: a cognitive framework for evaluation and design of usable authentication solutions. In: Internet Society. Wiley (2003). https://www.wiley.com/en-ad/Multiple+User+Interfaces:+Cross+Platform+Applications+and+Context+Aware+Interfaces-p-9780470854440
21. Seffah, A., Javahery, H.: Multiple User Interfaces: Cross-Platform Applications and Context-Aware Interfaces. Wiley (2014)
22. Garfinkel, S., Lipford, H.R.: Usable security, history, themes and challenges. Morgan and Claypool Publishers, San Juan (2014)