On Supporting Security and Privacy-preserving Interaction through Adaptive Usable Security

Marios Belk[1], Christos Fidas[1,2], Panagiotis Germanakos[1,3], George Samaras[1]

[1]Department of Computer Science, University of Cyprus, CY-1678 Nicosia, Cyprus
{belk,cssamara}@cs.ucy.ac.cy
[2]Interactive Technologies Lab, HCI Group, Electrical and Computer Engineering Department
University of Patras, GR-26504, Patras, Greece
fidas@upatras.gr
[3]SAP AG, Dietmar-Hopp-Allee 16, 69190 Walldorf, Germany
panagiotis.germanakos@sap.com

Abstract. The purpose of this paper is to propose a preliminary framework for supporting usable security on the World Wide Web through adaptivity in user interface designs. In particular we elaborate the concept of "Adaptive Usable Security" and suggest that it is a promising research area aiming to organize and present information and functionalities in an adaptive format to diverse user groups, by using different levels of abstractions through appropriate interaction styles, terminology, information presentation and user modeling techniques related to security and/or privacy preserving tasks. Furthermore, we present components of a preliminary framework aiming to provide guidance in developing "adaptive usable secure" interactive systems. The results and implications of this paper can be considered valuable in elaborating a common architecture for future deployment of adaptive usable security systems on a variety of application areas and services through the World Wide Web.

Keywords: Adaptive Interactive Systems, User Modeling, Usable Security

1 Introduction

Security and privacy issues of today's interactive systems are considered of paramount importance as it is known that the consequences of a security breach can harm the credibility and legal liability of an organization, decreases users' trust and acceptance while it exponentially increases maintenance and support costs. In this context, one of the most important and challenging issues is to support users, engaged on tasks related to security and privacy, through usable computer human interface designs.

In 2009, the U.S. Government acknowledged "usable security" as one of the eleven hard problems to be researched for achieving cyber security; usable security is a cross-layer issue correlating with all other hard problems related to cyber security which are: scalable trustworthy systems (including system architectures and requisite development methodology), enterprise-level metrics (including measures of overall

system trustworthiness), system evaluation life cycle (including approaches for sufficient assurance), combatting insider threats, combatting malware and botnets, global-scale identity management, survivability of time-critical systems, situational understanding and attack attribution, provenance (relating to information, systems, and hardware) and privacy-aware security [1]. Usable security is therefore pronounced as the cornerstone of future online services and applications which are expected to offer a rich set of computing and communication services to users in a broader context representing unprecedented opportunities to access, manipulate, and share information as well as to accomplish tasks through heterogeneous devices and contexts of use. Within this realm, adapting functionality and content, of an interactive system, into an assemblance that specific users are able to understand and use intuitively in order to perform specific tasks related to security or privacy issues is a challenging endeavor. It entails understanding and modeling human behavior for diverse user groups and stakeholders, with regards to structural and functional user requirements, which needs to be translated into usable computer human interaction designs and workflows, whilst minimizing user cognitive loads, perceptual and learning efforts aiming to minimize erroneous interactions. Indeed, an erroneous user decision related to security and privacy issues can unarm the most sophisticated security architecture.

Taken into consideration that users of the World Wide Web do not necessarily share common conventions, cultural, and cognitive backgrounds; tools and resources; and contexts in which security and privacy decisions are required to be taken we suggest that adaptive user interfaces [2] (Figure 1) provide a viable alternative in order to ensure usable security and privacy offering equal chances for participation by all. Adaptive user interfaces in the context of usable security provide an alternative to the "one-size-fits-all" approach of static user interfaces by adapting the interactive system's structure, navigation, terminology, functionalities and presentation of content to users' perceptions and level of knowledge with regards to security and privacy related tasks, aiming to increase the usability and provide a positive user experience.

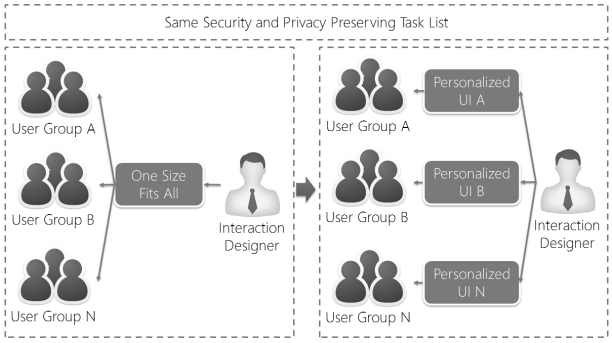

Fig 1. Adaptive User Interfaces in Usable Secure Systems.

The paper is organized as follows: Section II elaborates on the notion of adaptive usable security. Section III proposes a preliminary framework and presents an example of applying the framework in the frame of an online banking system. Finally, Section IV concludes the paper and describes directions of future work.

2 Adaptive Usable Security

The notion of usable security has been the subject of numerous research papers since the World Wide Web's exponential growth, and user interface experts have performed several attempts to provide an intuitive way of computer human interaction related to security and privacy preserving tasks [3-7]. However, usable security is still an open research area mainly due to lack of understanding in depth security and privacy tasks and integrating them intuitively in the user interface design process by following a User Centered Approach [7]. User-centered design approaches focus on interacting iteratively with the end-users, especially for identifying and validating user requirements, designing system prototypes as well as for evaluating them. The aim is to investigate thoroughly what users require from a system design and how the system can support them in accomplishing specific tasks effectively, efficiently, and with a certain degree of user satisfaction. An important aspect of this process is to model a user interaction with a user interface. A good design practice aims to establish a common ground among designers and users related to aspects of user-system interaction by formalizing the information architecture of the interactive system and specify the interaction flow for accomplishing specific tasks. A well-used and simple approach to modeling interactive systems is to analyze the user actions in several levels of abstractions and identify on each level the most appropriate terminology, content presentation and interaction flow.

Ineffective practice of usable security, ignore to naturally embed in the system's design, security and privacy issues, and usually adopts a "one size fits all" approach when concerning user interface designs ignoring the fact that different users develop different structural and functional mental models and thus need individual scaffolding. Forming a mental model related to system interaction embraces a seven step iteration cycle [8]. The users form a conceptual intention related to their goal and try to adapt the intention to the features provided by the system and from these, user-perceived features the users try to perform their actions. Subsequently, the users attempt to understand the outcome of their actions by evaluating the system response. The last three stages help the users develop and refine their mental models of the system. The whole process is repeated in iterations of user actions and evaluations which results in developing and refining their mental models by interpreting the system's response. The development and maintenance of user mental models is a dynamic and continuous process, especially related to novice and average users who are still in the process of developing these models based on empirical system interaction. Once these models are created, then the users interact with the system in more automated ways, faster, and more efficiently.

Within this context, supporting usable security of interactive systems with user-adaptive technologies is based on the promise that understanding and modeling human behavior in terms of structural and functional user requirements related to security or privacy preserving tasks can provide an alternative to the "one size fit all" approach aiming to formalize and specify appropriate user modeling that deals with what information is important to be incorporated in the user model and how to represent and extract this information, as well as formalize and specify appropriate adaptation types and mechanisms, and how to communicate them to the adaptive user interfaces in order to improve the system's usable security and user experience.

3 A Preliminary Framework for Adaptive Usable Security

Following a User-Centered Design (UCD) approach the first step of a framework which utilizes the development of an adaptive usable secure interactive system is to identify the user categories and group them according to predefined criteria which are considered to affect interaction design related to usable security. These grouping criteria, can be related with the static or dynamic part of the user or context information model, and need to be identified and specified for each application area as each specific domain embraces its own constructs, user affordances and custom requirements and thus requires to be modeled explicitly. This is further strengthened taking into consideration that usable security has different semantics and specifications in various application areas on the World Wide Web, e.g., e-banking, e-government, e-health, e-gaming, e-entertainment. As an example, providing an adaptive usable security solution to an on-line banking system is a different challenge than providing an adaptive usable security solution to an on-line stock exchange system as in both systems tasks, user groups, terminology and affordances are very different. Thus, it becomes obvious that supporting this attribute needs a modular approach embracing different levels of abstractions related to security and privacy issues that needs to be modeled in each application area explicitly.

Taking into consideration that security and/or privacy preserving tasks are usually secondary tasks which are performed by the users combined with the primary tasks, it becomes mandatory to scaffold this tasks with more sophisticated approaches. In this context, defining appropriate information architecture together with efficient, and effective user interface designs are necessary steps for allowing users to navigate logically through an interactive system and performing intuitively security or privacy preserving tasks in an efficient and effective way with respect to their own individual preferences. This is achieved at early stages of user requirements analysis by defining an appropriate information architecture in terms of organizing, grouping and presenting information, data and results in an understandable format to diverse user groups, by using adaptive content presentation with different levels of abstractions through appropriate interaction styles, terminology and information presentation techniques related to security or privacy preserving tasks. For each task, which affects the security and/or privacy policy, it is proposed to enrich the user interface with valuable information aiming to improve the level of information security awareness for each user category in an appropriate approach based on user and context information.

The proposed framework consists of three main layers; *the security application layer*, *the adaptation layer*, and *the adaptive user interface layer*.

The security application layer identifies specific and important attributes that are dependent on each application domain. As mentioned previously, each application domain has customized requirements with regards to adaptive usable security. In this respect, the security application layer includes the identification of *user categories*, *user model features* (i.e., user and/or context information), *tasks* and *security and privacy implications*, and *adaptation goals* of the adaptive usable security system.

The *user category* dimension supports the classification of user groups according to predefined criteria which are considered to affect interaction design related to usable security.

The *user model* dimension indicates what characteristics of the user could be used as a source of adaptation, i.e., to what characteristics of the user the system can adapt its behavior. The *security and privacy related tasks* indicate what could be adapted in the system, i.e., which features of the system can be different for different users. It is argued that system designers should list the tasks the users are supposed to accomplish through system interaction and analyze these tasks through task analysis techniques, taking into consideration the security and privacy aspects of interaction in order to understand cognitive processes that take place during task completion and may affect security and privacy issues. Given this analysis, the *adaptation goals* should be identified aiming to offer personalized adaptation effects related to security awareness information to specific user categories through appropriate adaptation mechanisms.

The adaptation layer specifies which mechanisms are appropriate for the adaptation of security and privacy related tasks. Simple user customization and rule-based mechanisms could be used to decide what adaptation will be performed on the content and functionality of the system. For example, users could customize the structure and complexity of privacy related tasks. Furthermore, it is argued that collaborative mechanisms [9] could assist the adaptation process by modeling the behaviour of users with similar preferences.

The adaptive user interface layer is responsible for deciding which features of the interface (information architecture or functionality) should be adapted and how the adaptation effect should be transformed into a usable user interface design for improving the system's security. Various adaptive content presentation techniques could be used to provide personalized tasks to the users, such as, expanding/collapsing content fragments based on the user's level of knowledge on security/privacy terminology, or altering the presentation of content based on users' cognitive styles (i.e., Imager/Verbal styles) [10]. Adaptive navigation support could also assist security and privacy related tasks by guiding the user through a security related task, by restricting navigation space to complex tasks, or by augmenting security related tasks with additional information about the task, with appropriate annotations.

3.1 Example of Applying the Framework in an Online Banking System

World Wide Web services and applications entail in their interaction design high quality and extensive security measures aiming to protect themselves and their users from miscellaneous interactions. This includes, for example, ensuring that confidential data sent over the internet cannot be accessed or modified by unauthorized third parties. Typical threats in such contexts are related to deleting or tampering data while they are being transmitted or gaining unauthorized access to system resources or accounts through a variety of techniques such as viruses, trojans, phishing, or hacking.

Within this context, users are expected to perform various tasks related to security, which include, among others, properly configure an antivirus or firewall software, configure browser's security settings, installing certificates, confirm the credentials of the Web server by an independent certificate authority, be aware of hacking tricks such as phishing ("password fishing"), choose secure, difficult to remember passwords. In this realm, user studies revealed the average users either ignore security

indicators, such as absence or invalidity of SSL certificates [11] or cannot easily detect and understand this practice and its consequences [12].

We next present and discuss an example of applying the framework for adaptive usable security in an online banking system. In this context, user categories are grouped formed on the user's level of experience in online commercial transactions, such as novice users that use online banking tasks rarely, and expert users that use online banking tasks more often as we assume that expert users have already built their mental models relating to the system usage and need thus less scaffolding and education relating to security tasks.

Table 1. Specification of online banking attributes.

Task	Security/Privacy Implications	User Model	Adaptation Goals	Adaptation Mechanism
Login	User Authentication and Authorization	Location, Expertise, Interaction History	Additional support	Rule-based
Configuration	Security/Privacy Configuration	Goals, Knowledge, Background	Increase comprehension	Rule-based, Collaborative
Monetary Transaction	Security Certificates	Goals, Knowledge, Background	Provide security information awareness on certificates	Rule-based, Content-based
Login, Forum	CAPTCHA	Lingual/cultural context	Improve CAPTCHA usability	User customization, Rule-based

The user model incorporates user and context information such as the level of knowledge and background on security and privacy related tasks, individual traits (e.g., cognitive styles), platform characteristics (e.g., device characteristics, bandwidth) and lingual and cultural context characteristics. Primary security and privacy tasks of online banking systems include among others login mechanisms, configuration of security and privacy related settings, and monetary transactions. Table 1 summarizes the attributes of the framework for some of the tasks related to online banking interactions aiming to provide a proof of concept of the proposed framework. It is beyond the aim of this paper to provide an extensive and detailed paradigm on how the proposed framework can be applied in the online banking domain.

In this context some important user tasks related to security are the user authentication and authorization tasks which entail a rule-based adaptation mechanism that is used to assess the user's expertise and interaction history with the system by tracking the number of login attempts. The number of login attempts indicates the system to automatically offer security information awareness to the user or appropriate live customer support option to users who could not succeed to login in the system for several times. Furthermore, CAPTCHA [13] challenges which are required during failed login attempts aiming to provide a high confidence proof that it is a human being trying to gain access to the system, are adapted to user's lingual and cultural context [14] by utilizing simple user customization techniques and rule-based mechanisms (i.e., user indicates through a checkbox that (s)he prefers localized CAPTCHAs).

During monetary transactions, security certificate installation processes take into consideration the user's current goal or level of knowledge on certificates with the use of a weighed knowledge model that indicates the level of knowledge on specific security/privacy related terms. Based on this information about the user, the certificate is augmented with additional information, in the form of annotations in order to increase the comprehension of the security certificate. Content-based mechanisms [15] are also used to create a vector of keywords of the certificate and compare them with the user's weighed knowledge model to augment the security/privacy terms, that the user is not familiar, with additional information.

4 Conclusions and Future Work

In this paper a preliminary framework is proposed for supporting the design and deployment of usable and secure interactive systems driven primarily by the need to define more effective and efficient User-Centered Design (UCD) techniques related to usable security. It is argued that for supporting efficient and effective usable security, research in this area should partially move its focus away from the technical issues towards understanding the end users and developing approaches which can be applied in offering better awareness on security and privacy issues on an application domain, user and task level.

Within this realm the concept of adaptive usable security is elaborated with the aim to offer personalized security information awareness, to specific group of users who are engaged in accomplishing specific tasks within certain application domains, by rendering the information architecture and adapting its functionality based on user preferences and contexts of use. Adaptive usable security implies the ability of an interactive system to support its end users, who are engaged in security and/or privacy related tasks, based on user models which describe in a holistic way what constitutes the user's physical, cognitive and social context in which computation takes place. Such an approach facilitates, among others, reasoning of context-based rules which describe in a declarative way conditions which are considered important and need further investigation, scaffolding or detailed analysis by the designer.

The added value of the proposed framework relies on the fact that it speeds up the integration and adaption process of usable security by separating domain knowledge from the operational knowledge by describing a multilayer formal context model aiming to provide a common representation of contextual information, facilitating thus usable security aspects of an interactive system.

The aim of this paper is to increase our understanding and knowledge on supporting usable security interaction design through user modeling, and adaptivity in user interfaces based on adaptation mechanisms. Taking into consideration that future World Wide Web interactive systems will embrace a variety of factors affecting security and privacy issues across various application domains (like e-banking, e-government, e-health etc.) approaches like the proposed one can be of general value. Achieving usable security in future interactive systems will have wider social and economic impact by helping citizens to understand and familiarize with secure services and best practices for security and privacy on interactive systems which will offer a rich set of computation and communication services.

Future work, consist in developing suite of methods and techniques for understanding user attitudes and perceptions towards security and privacy issues in various application areas, transforming them into software specifications, designing and finally evaluating appropriate adaptive user interface designs in different contexts of use.

Acknowledgements. The work is co-funded by the PersonaWeb project under the Cyprus Research Promotion Foundation (ΤΠΕ/ΠΛΗΡΟ/0311(ΒΙΕ)/10), and the EU project SocialRobot (285870).

REFERENCES

1. Department of Homeland Security: A Roadmap for Cybersecurity Research. Available online http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf (2009)
2. Brusilovsky, P., Kobsa, A., Nejdl, W.: The Adaptive Web: Methods and Strategies of Web Personalization. Springer, Heidelberg (2007)
3. Adams, A., Sasse, M.A.: Users Are Not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Measures. J. Communications of the ACM. 42(12), 40-46 (1999)
4. Cranor, L., Garfinkel, S.: Security and Usability. O'Reilly Media, Inc. (2005)
5. Shay, R., Kelley, P., Komanduri, S., Mazurek, M., Ur, B., Vidas, T., Bauer, L., Christin, N., Cranor, L.: Correct Horse Battery Staple: Exploring the Usability of System-assigned Passphrases. In: ACM Symposium on Usable Privacy and Security, Article 7, 20 pages. ACM Press, New York, NY (2012)
6. Biddle, R., Chiasson, S., van Oorschot, P.: Graphical Passwords: Learning from the First Twelve Years. J. ACM Computing Surveys 44(4), 41 pages (2012)
7. Fidas, C. A., Voyiatzis, A. G., Avouris, N. M.: When security meets usability: A user-centric approach on a crossroads priority problem. In: Proc. of Panhellenic Conference on Informatics. PCI'10. IEEE Computer Society, 112-117 (2010)
8. Norman, D.: The Design of Everyday Things. Psychology of Everyday Action. New York (1988)
9. Su, X., Khoshgoftaar, T.: A Survey of Collaborative Filtering Techniques. J. Advances in Artificial Intelligence, Article 4, 19 pages (2009)
10. Riding, R., Cheema, I.: Cognitive Styles – An Overview and Integration. J. Educational Psychology 11(3-4), 193-215 (1991)
11. Schecter, S. E., Dhamija, R., Ozment, A., and Fischer, I.: The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies. In Proc. of IEEE Symposium on Security and Privacy (2007)
12. Falk, L., Prakash, A., and Borders, K.: Analyzing Websites for User-Visible Security Design Flaws. In Proc. of Symposium on Usable Privacy and Security. ACM Press, 117-126 (2008)
13. von Ahn, L., Blum, M., Langford, J.: Telling Humans and Computers Apart Automatically. J. Communications of the ACM 47, 56-60 (2004)
14. Fidas, C., Voyiatzis, A., Avouris, N.: On the Necessity of User-friendly CAPTCHA. Proc. of Human Factors in Computing Systems (CHI 2011), pp. 2623–2626, ACM Press (2011)
15. Smyth, B.: Case-based Recommendation. In: The Adaptive Web, Brusilovsky, P., Kobsa, A., Nejdl W. (Eds.), Springer-Verlag, pp. 342-376 (2007)