UDC 004.055 + 004.056

I.V. Guchenko

USABILITY ASPECT OF INFORMATION SECURITY SYSTEMS

The article is devoted to the problem of usability of information security systems. Importance of usability for successful conducting of security tasks by users is shown. Usability security principles have been analyzed. Investigation of usability issues associated with information security-related tasks is conducted. Descriptions of the demands imposed on the users by each method of corresponding security task are compared with definitions of usability properties. The research on types of relations between usability properties and information security tasks is made. Future implication of the research results is shown.

Key words: *software usability, security, information security system, security task, user, usability properties.*

Introduction

Usability is an important characteristic of any product that is used by a customer. This applies to software, in particular to information security systems. On the one hand, high usability level of a system allows users to accomplish security tasks with effectiveness, efficiency and satisfaction in a specified context of use. On the other hand, such usability can reduce the ability of information security system to defend against adverse impacts. That is why it is important to establish the types of relations between usability issues and security tasks. It will help to find the compromise solution during the development of usable (with sufficient usability level) information security system.

Literature analysis

The main purpose of information security systems is to defend against adverse impact. In many cases the weakest link of such a system is represented by the human operator. Security systems must be viewed as socio-technical systems that depend on the social context in which they are embedded to function correctly [1]. They will only be able to provide the intended protection when people actually understand and are able to use them correctly. There is a big difference between the degree by which systems can be considered theoretically secure (assuming they are correctly operated) and actually secure (acknowledging that often they will be operated incorrectly). In many cases, there is a trade-off between usability and theoretical security. But some authors maintain that theoretical security does not have to be compromised if usability aspects are considered from the beginning of the system development life cycle [2, 3]. This represents the *sustaining approach* to creating user-friendly security because it does not question the underlying security building blocks, only how they are implemented. However, there are always certain security blocks, which are inherently unsuitable for designing user-friendly security solutions. In that case some authors are talking about the *disruptive approach* which questions the applicability of existing security primitives, and seeks to replace them with other primitives that better support user friendly security [4]. In both approaches, there is a need for understanding the security usability (usability of security) principles. In [5] a set of general security usability principles were proposed: security action and security conclusion usability principles. These principles were used for vulnerability analysis and risk assessment in [6].

<u>Security action usability principles:</u>

– users must understand which security actions are required of them;

- users must have sufficient knowledge and the ability to take the correct security action;
- the mental and physical load of a security action must be tolerable;
- the mental and physical load of making repeated security actions for any practical number of instances must be tolerable.

Security conclusion usability principles:

- user must understand the security conclusion that is required for making an informed decision;
- the system must provide the user with sufficient information for deriving the security conclusion;
- the mental load of deriving the security conclusion must be tolerable;
- the mental load of deriving the security conclusions for any practical number of instances must be tolerable.

In [7] the following properties of security usability are represented:

- Abstraction: this is a system of abstract rules for deciding whether to give access to resources. UI design will need to take this into consideration;
- Lack of feedback: a system security configuration is usually complex, and attempts to summarize it are not adequate;
- Weakest link: users need to be trained or guided in all aspects of security of their system;
- Unmotivated user: security is usually secondary goal to users;
- Limited human skill: usable design must take into account what humans do well and what they don’t.
-

Grounding

The major types of security controls that exist today apply to the following areas: identification and authentication, data integrity, data confidentiality, data availability, system integrity and intrusion detection [8]. Many different security control methods [8] involve interactions between humans and computer hardware and software, yet they were largely developed with little regard for usability. Because the degree of security provided by the various security control methods typically depends on the actions of system administrators and end-users, security hinges on the usability. Consequently, there is a critical need to focus on investigation of usability issues associated with information security-related tasks. There is a detailed taxonomy of information security tasks and the associated usability issues in [8].

Previous author’s works are devoted to the development of the method and the tool of software product usability management [9]. The method is based on automated multi-criteria usability evaluation. The model of usability evaluation based on the method of nested scalar convolutions and is represented by a scalar function of the additive convolution. It supports usability management of software products based on the automated evaluation of users’ feedback. Usability is represented as a four-level hierarchical system of usability criteria. It is decomposed on subcharacteristics, each of which – on corresponding properties, and properties – on measures. Such decomposition is based on the relevant standards, guidelines, expert judgments etc. Usability subcharacteristics from ISO / IEC 25010:2011 were applied [10]. List of properties was developed using QUIM model [11].

The aim of the present article is to determine the connection of information security tasks with usability properties. As a result, it will be possible to predict the effect of the growing value of usability on security.

Case study. The information about the nature of the security task and corresponding methods are taken from [8]. We compare included descriptions of the demands imposed on the users and system administrators by each security method with definitions of usability properties from [9]. Results are pointed in Table 1, where inversely proportional relation is denoted as ● and directly proportional relation – as ○. Some explanations are given below.

Identification and Authentication.

1. Password entry: a) require user to maintain and act on knowledge that is sometimes detailed. Such requirement is opposite to the Minimal Action property definition [9]; b) high memory demand is inversely proportional to the Minimal Memory Load property; c) password may impose unnatural syntactic and other constraints (e.g. minimum password length) that reduce the Simplicity.

Table 1.

Interactions between usability properties and information security tasks.

Usability properties	**Information security tasks**					
	Identification & Authentication	Integrity, Confidentiality, and Availability of Data	Intrusion detection	Responding to Intrusions	Assurance of Operational Continuity	General usability
Time behavior		○				
Attractiveness			○	○	○	
Likeability	●	○				
Flexibility	●	○				
Minimal action	●	○				
Minimal memory load	●	●	○	○	○	
User guidance	●	○	○	○	○	
Consistency	●	○				
Self-descriptiveness	●	○				
Feedback		○	○	○	○	
Accuracy		○				
Fault-tolerance		○				
Readability	●	○				○
Controllability	●	○				
Navigability	●	○				
Simplicity	●	○	○	○	○	○
Familiarity			○	○	○	
Guide						○
Demonstrations						○
Help						○

2. Biometrics and physiological approaches often are not user friendly and cause the increasing of user’s anxiety. Thus, Likeability value is decreasing.
3. Physiological approach sometimes is not comfortable for certain populations, such as handicap people, shorter and taller persons. In such a case, it contradicts the Accessibility definition. Accessibility is a usability subcharacteristic that includes the

following properties: flexibility, minimal action, minimal memory load, user guidance, consistency, self-descriptiveness, readability, controllability, navigability and simplicity [9].

Integrity, Confidentiality, and Availability of Data.

Corresponding methods of this information security task require from users to be able to: understand and recognize the commands and options, use the commands in an appropriate way, remember keys used in digital signatures [8]. Mentioned abilities are connected with Accessibility and Operability subcharacteristics of usability. Operability includes time behavior, consistency, feedback, fault-tolerance and controllability [8]. Properties of Accessibility were mentioned earlier. Only Minimal memory load has inversely proportional influence on considered task, high value of other properties increase the quality of information security task performed by the user.

Intrusion Detection, Responding to Intrusions, Assurance of Operational Continuity.

1. User should be informed about the internal state of a system. The warning or error messages must be detailed but specific including a suggested corrective action for some security problem, and links to obtain additional information or external assistance. All these demands increase values of User Guidance and Feedback properties of usability.
2. Only relevant security information should be displayed, technical terms should be avoided as much as possible, security activities must be easy to realize and understand. Thus, we have directly proportional relation to Simplicity and Minimal Memory Load properties.
3. In some cases, it is convenient to present important security concepts to the user in an entertaining manner. In that case, Attractiveness of a system will be better.
4. Using of figures or pictures helps to convey the available security features to the user clearly and appropriately. It affects directly on Familiarity property of usability.

General usability.

1. Displayed information should be readable, legible, clear and understandable. Providing of high Readability and Simplicity level increase general usability of a system without reducing its security.
2. User should be able to: understand the instructions and take the appropriate steps; acquire knowledge about the system by reading the instructions, performing training tutorials etc.; have sufficient knowledge on the type of information displayed; be able to use the shortcuts that system provides to accomplish the task quicker. Mentioned abilities directly depend on Guide, Demonstration and Help properties of usability.

Conclusion

Many significant risks are caused by poor usability of information security systems. In earlier author's works, the method and the tool of software usability management were represented. The purpose of using the method is to create a product that meets user expectations. It allows to control reasonably the software usability level taking into account development resources as optimization criteria. In a case of the information security system the method and the tool can help to create software product that allows users to accomplish security tasks with effectiveness, efficiency and satisfaction in a specified context of use. Achieving of satisfied usability level is connected with increasing of usability properties' values. But it is very important to understand how increasing usability will affect on security of the system. This issue was explored in the article. Author made a research on types of relations between usability properties and information security tasks. Further work will be devoted to the modification of the method and the tool of usability management in order to create usable security systems.

References

1. Sasse M.A. Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery / M.A. Sasse // CHI'2003: Human Factors in Computing Systems: proceedings. – 2003. – P. 324-338.
2. Sasse M.A. Usable Security: What is it? How do we get it? / M.A. Sasse, I. Fleshais // Security and Usability: Designing Secure Systems that People Can Use. – O'Reilly, 2005. – P. 234-241.
3. Dourish P. An Approach to Usable Security Based on Event Monitoring and Visualization / P. Dourish, D. Redmiles // New Security Paradigms Workshop: proceedings. – ACM Press, 2002. – P. 75-81.
4. Smetters D. Moving from the design of Usable Security Technologies to the Design of Useful Secure Applications / D. Smetters, R. Grinter // New Security Paradigms Workshop: proceedings. – ACM Press, 2002. – P. 82-89.
5. Josang A. Usability and Privacy in Identity Management Architectures / A. Josang, M. AlZomai, S. Suriadi // Australasian Information Security Workshop: proceedings. – 2007. – Vol. 68. – P. 502-517.
6. Security Usability Principles for Vulnerability Analysis and Risk Assessment / Josang A., AlFayyadh B., Grandison T [et.al] // Annual Computer Security Applications Conference: proceedings. – 2007. – P. 473-482.
7. Usability and Security. An Appraisal of Usability Issues in Information Security Methods / E. Shultz, R. Proctor, Mei-Ching Lien [et.al] // Computer and Security. – Elsevier Science Limited, 2001. – Vol.20(7). – pp. 620-634.
8. Гученко І.В. Метод і засіб управління зручністю використання програмних продуктів: дис. ... кандидата технічних наук : 01.05.03 / Гученко Інна Володимирівна. – К., 2012. – 124 с.
9. Systems and software engineering, Systems and software Quality Requirements and Evaluation (SQuaRE), System and software quality models: ISO/IEC 25010:2011. – Geneva: International Organization for Standardization /International Electrotechnical Commission, 2011. – 34p.
10. Padda Harkirat K. QUIM: A Model for Usability/Quality in use Measurement / Harkirat K. Padda. – Colne: Lambert Academic Publishing, 2010. – 124 p.

Стаття надійшла _18_._04_._2014___
Прийнято до друку _06_._05_._2014___

Анотація

Гученко Інна Володимирівна

Системи безпеки інформації в аспекті зручності використання програмного забезпечення

Стаття присвячена проблемі зручності використання систем інформаційної безпеки. Показано важливість зручності використання програмного забезпечення для успішного виконання користувачами задач безпеки інформації. Проаналізовано принципи зручності використання, пов'язані з безпекою. Досліджено проблемні питання зручності використання програмного забезпечення, що впливають на виконання завдань інформаційної безпеки. Проведено зіставлення вимог, що накладаються на користувачів при застосуванні відповідних методів виконання задач безпеки інформації, з визначеннями властивостей зручності використання програмного забезпечення. Досліджено види залежностей між чисельними характеристиками властивостей зручності використання та якістю виконання завдань інформаційної безпеки. Вказано майбутнє застосування результатів дослідження.

Ключові слова: *зручність використання програмного забезпечення, безпека, система безпеки інформації, завдання безпеки, користувач, властивості зручності використання.*

Аннотация

Гученко Инна Владимировна

Системы безопасности информации в аспекте удобства использования программного обеспечения

.

Статья посвящена проблеме удобства использования систем информационной безопасности. Показана важность удобства использования программного обеспечения для успешного выполнения пользователями задач безопасности информации. Проанализированы принципы удобства использования, связанные с безопасностью. Исследованы проблемные вопросы удобства использования программного обеспечения, которые влияют на выполнение задач информационной безопасности. Проведено сопоставление требований, налагаемых на пользователей при применении соответствующих методов выполнения задач безопасности информации, с определениями свойств удобства использования программного обеспечения. Исследованы виды зависимостей между численными характеристиками свойств удобства использования и качеством выполнения задач информационной безопасности. Указано будущее применения результатов исследования.

Ключевые слова: *удобство использования программного обеспечения, безопасность, система безопасности информации, задачи безопасности, пользователь, свойства удобства использования.*