Usable Security Versus Secure Usability: an Assessment of Attributes Interaction

Oleksandr Gordieiev[1], Vyacheslav Kharchenko[2] and Kate Vereshchak[3]

[1]Banking University, 1 Andriivska Street, Kyiv, Ukraine
alex.gordeyev@gmail.com
[2]National Aerospace University «KhAI», 17 Chkalova Street, Kharkiv, Ukraine
V.Kharchenko@csn.khai.edu
[3]Luxoft, 10/14 Radisheva Street, Kyiv, Ukraine
vereshchak@gmail.com

Abstract. Attributes of information systems quality described in standard ISO/IEC25010 (2010) are analyzed. Some of them are contradictory, dependent and competing. One of the most competing characteristics are usability and security (U&S). The article considers two main aspects of U&S interaction called "usable security" and "secure usability". The technique of qualitative assessment of the U&S interaction based on analysis of subcharacteristics and metrics is suggested. An example of the technique application to assess U&S interaction for university web-site is discussed.

Keywords. Usability and security interaction, usable security, secure usability ISO/IEC25010, ISO/IEC25023

Key Terms. Usability, security, software characteristics, software metrics, interaction

1 Introduction

1.1 Motivation

Information systems are characterized by a set of characteristics/attributes that are defined by international standards. The standard ISO/IEC 25010 «System and software quality model» [1] defines the following 10 characteristics of information systems: functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, portability. Such nomenclature was formed in result their evolution during about 60 years [2]. Certain characteristics (subcharacteristics) of information systems interact at each other. I.e. there are situations when strengthening (weakening) of one of the characteristics requires or generates strengthening (weakening) of another or even a group of information

systems. In the article we will consider a couple of the most important, mutually influence and competitive characteristics – usability and security (U&S).

1.2 State of Art

First of all, we need give of description for U&S attributes. Usability – degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use [1]. Security - degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization [1]. Information systems must have of Usability and Security characteristics, because they must be comfortable in use and secure simultaneously. Depending on field of information systems application, levels of U&S requirements and characteristic values are not the same. In most cases, information systems are more usable, including at the expense of security, or more secure at the expense their usability.

Problems of U&S characteristics interaction are well known, researched and presented in materials of conferences, in articles and books. Analysis of works in this field gave us possibility make some conclusions and divide of accessible works on following groups in some fields:

- most part of works are about concrete problems in U&S field and mechanisms for their solutions [3, 4, 5, 6, 7]. In particular, in [3] are viewed alphanumeric passwords problems and are presented ways for their decision;
- following group of works about general conceptual questions in the U&S field [8, 9];
- part of works about problems and peculiarities of U&S interaction on required levels [6], on processed levels [10, 11] and on model levels (including UML models) [12];
- small group includes works about U&S problems for mobile applications [13,14];
- separate works about analysis of literature in U&S problems field [15];
- some articles about U&S characteristics evolution. Authors of such works represent the evolution and interaction of usability and security characteristics [16, 2].

1.3 Goal and Structure

Preliminary analysis of works in U&S field permitted to make the following conclusions and determine goal of the paper:

- firstly, characteristics of U&S which described in last program engineering standards [1, 17, 18] are one from other results of 40 years evolution [2, 16]. They represented as complex characteristics with set of depended subcharacteristics;
- secondly, analysis of U&S subcharacteristics and metrics did not conduct in existing works [3-16], which describe problems interaction of U&S characteristics;
- thirdly, separate subdivision was organized at National Institute of Standards and Technology (NIST) of USA [20], which solves tasks of U&S interaction.

However, well known works describe, first of all, influence of Usability on Security and did not take into account aspects of influence on level of their subcharacteristics.

Thus, **goal** of article is determination, analysis and assessment of U&S interaction on subcharacteristics and metrics levels.

The paper has the following structure. Main second section contains:

- description of "Usable security" and "Secure usability" interaction problem;
- analysis of U&S interaction on subcharacteristics level and variants U&S subcharacteristics interaction;
- analysis of U&S interaction on metrics level.

The third section analyses and assesses U&S interaction for university web-site and the fourth section concludes and describes directions of the future research.

2 Usability and Security

2.1 Two Sides of the Same Coin

Exist of two possible aspects of research and development (i.e. two sides of the same coin): usable security and secure usability. Let's consider in more details what are the differences between these two aspects.

Usable Security

First aspect gives an answer on a question: how to develop functions secure access to resources such, in order to ensure acceptable/necessary level of usability of user interfaces. In order to link of U&S characteristics in the usable security aspect was more understandable, we need represent example of such an interaction. Very often procedure of registration on web-site requires from users to confirm their presence near personal computer. It needs to exclude automatic registration on the Internet. As a rule, web-site offers to users input data for CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) [20]. In majority of cases, the CAPTCHA is information, which automatic generator on picture of web-page and which necessary input to textbox. Sometimes users have problems with input of information from CAPTCHA (i.e. have problem with Public Turing test), because information which is represented on picture periodically cannot be discernible. (Fig. 1). Defect of such technique of identification can provoke discomfort for user. For solution of such problem user necessary, periodically manually reload the picture of CAPTCHA waiting for recognizable information. User can wait long time of appearance recognizable information. User can also delay or cancel, for example, web-site registration procedure. This is an example, when «complex» security kills usability – (cSkU) Information systems developers necessary take into account such aspect, when they make project of user interfaces. We have to exclude situation, when high level of security «kills» the usability.

It should be noted, that subdivision at National Institute of Standards and Technology (NIST) of USA researches such U&S problems [19].

Fig. 1. Examples of CAPTCHAs.

Secure Usability

Second aspect has relationships with development of user interfaces thus, in order to ensure necessary level of information security. Lets describe an example of such interaction between usability and security. Public Turing test can be maximum simple and represents one checkbox element, which necessary will set up in significance «check» (Fig. 2). From usability position such variant of Public Turing test is more better than his variant on Fig 1. But from security position such variant (Fig. 2) is more worse, because as against previous variant (Fig. 1) such variant is more simply pass (by software bots) during automatic registration without user. In other words, in such a context there is another competition. This is situation, when «simple» usability "kills" security – sUkS).

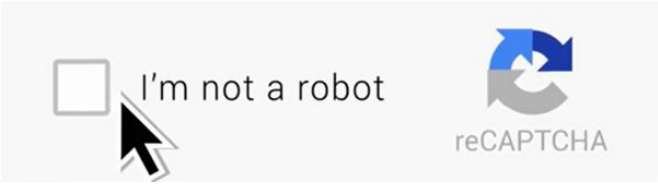

Fig. 2. More simple Public Turing test.

2.2 Criteria

General

Thus, U&S characteristics really have interconnection in the form of two aspects and formally differences can be described through «castle» of objective function and limitations.

– in first case it is necessary to ensure the required level of usability (Ureq), at that maximize of security (Smax), i.e. $S \rightarrow max$, $U \geq Ureq$;

– in second case it is necessary ensure the required level of security (Sreq), at that maximize of usability (Umax), i.e. . U→ max, S ≥ Sreq.

We pay attention, that U&S characteristics and their sub characteristics described in article as their interpretation in group of standards ISO 25000.

Attributes of Security and Usability

Examined positions can be represented out in detail as:

– security – is combination of following subcharacteristics [1]: confidentiality, integrity, non-repudiation, accountability and authenticity

$$S = \{Conf, Integr, N\text{-}rep, Acc, Aut\};$$

– usability – is combination of following subcharacteristics [1]: appropriateness recognizability, learnability, operability, user error protection, user interface aesthetics, accessibility.

$$U = \{AppRec, Learn, Oper, UEP, UIA, Acs\}.$$

2.3 U&S Subcharacteristics Interaction Analysis

We will consider interaction between U&S subcharacteristics. For that we will describe more detail formulations their subcharacteristics [1], which represented in table 1.

Table 1. U&S subcharacteristics formulations.

№	Characteristics (subcharacteristics)	Description
1	Usability	degree eto which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use
1.1	Appropriateness recognizability	degree to which users can recognize whether a product or system is appropriate for their needs
1.2	Learnability	degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use
1.3	Operability	degree to which a product or system has attributes that make it easy to operate and control
1.4	User error protection	degree to which a system protects users against making errors
1.5	User interface aesthetics	degree to which a user interface enables pleasing and satisfying interaction for the user
1.6	Accessibility	degree to which a product or system can be used by people with the widest range of characteristics

		and capabilities to achieve a specified goal in a specified context of use NOTE 1 The range of capabilities includes disabilities associated with age. NOTE 2 Accessibility for people with disabilities can be specified or measured either as the extent to which a product or system can be used by users with specified disabilities to achieve specified goals with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use, or by the presence of product properties that support accessibility.
2	Security	degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization
2.1	Confidentiality	degree to which a product or system ensures that data are accessible only to those authorized to have access
2.2	Integrity	degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data
2.3	Non-repudiation	degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later
2.4	Accountability	degree to which the actions of an entity can be traced uniquely to the entity
2.5	Authenticity	degree to which the identity of a subject or resource can be proved to be the one claimed

We have received set of variants of U&S subcharacteristics interaction because of U&S subcharacteristics analysis. Set of variants of U&S subcharacteristics represents table 2.

We will comment received variants. First of all, we will set the numeration as two numbers (from table 2), which includes the first number as usability characteristic and the second number as security characteristic:

– 1-1. Appropriateness recognizability subcharacteristic has interaction with confidentiality subcharacteristic. It is obvious, because before ensuring `Confidentiality`, user must, for example, see text boxes for input confidential information and inputted such information;

– 1-2, 1-3, 1-4, 1-5. In authors opinion, such variants of interaction between U&S characteristics are possible, but they require additional research for set up more exact of interaction type;

Table 2. Variants of interaction of U&S subcharacteristics.

№	Usability characteristics/ Security characteristics	Confidentiality	Integrity	Non-repudiation	Accountability	Authenticity
		1	2	3	4	5
1	Appropriateness recognizability	↑↑/↓↓	?	?	?	?
2	Learnability	↑↓	–	–	–	–
3	Operability	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓
4	User error protection	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓
5	User interface aesthetics	↑↑/↓↓	?	?	?	?
6	Accessibility	↑↓	↑↓	↑↓	↑↓	↑↓
– - interaction is absent;						
↑↑ - increase of level of one characteristic incurring to increase of level of other characteristic;						
↑↓ - increase of level of one characteristic incurring to decrease of level of other characteristic;						
↓↓ - decrease of level of one characteristic incurring to decrease of level of other characteristic;						
? - interaction is exist, but type of interaction to set very difficult (exist necessity of additional research)						

– 2-1. Such variant of interaction between subcharacteristics Learnability and Confidentiality exists, because if user receives more information abaut Confidentiality, than the level will be lower. Thus, if level of Learnability will increase, level of Confidentiality will decrease. And vice versa, if level of Learnability will decrease, level of Confidentiality will increase;

– 2-2, 2-3, 2-4, 2-5. In authors opinion, such variants of interaction between subcharacteristics are absent;

– 3-1, 3-2, 3-3, 3-4, 3-5. Such variants of interaction between subcharacteristics of Operability and Confidentiality, Integrity, Non-repudiation, Accountability, Authenticity exist, because of increase of Operability level leads to increase in such subcharacteristics, and vice versa, because of decrease of Operability level leads to decrease such subcharacteristics;

– 4-1, 4-2, 4-3, 4-4, 4-5. Variants of interaction between User error protection and Confidentiality, Integrity, Non-repudiation, Accountability, Authenticity exist, because decrease of count of user errors incurring to increase of level of characteristics Confidentiality, Integrity, Non-repudiation, Accountability and Authenticity, but increase of count of user errors incurring to decrease their level;

– 5-1. User`s interface aesthetics subcharacteristic has interaction with Confidentiality subcharacteristic, because, when user works with information systems interface, which has attractive design and well tidy colors, user has esthetical satisfaction, consequently, he can see textboxes for input confidential information and input her;

– 5-2, 5-3, 5-4, 5-5. In authors opinion, such variants of interaction between U&S subcharacteristics are possible, but require additional research for set up more exact of interaction type;

– 6-1, 6-2, 6-3, 6-4, 6-5. In this variants if the level of Accessibility characteristic will increase then levels of all subcharacteristics of security characteristic will decrease and vice versa, if level of Accessibility characteristic will decrease then levels of all subcharacteristics of security characteristic will increase. It is obvious, because of ensuring of Accessibility characteristic in information systems for people with disabilities in user`s interfaces it is necessary to do coordinal redesign of user interfaces. As a rule, such redesign of interfaces, on the one hand, lighten of interaction with software for people with disabilities, on the other hand, it is source of level decrease for all subcharacteristics of security characteristic.

2.4 U&S Metrics Analysis

We will analyze of U&S metrics. For that, first of all, we will represent short description of metrics and primitives (table 3).

Table 3. Brief description of U&S metrics.

№	Name of metric	Description	Primitives	Characteristics/ Subcharacteristics
1.	Description completeness	What proportion of functions (or types of function) are described as understandable in the product description?	A= Number of functions (or types of functions) described as understandable in the product description B= Total number of functions (or types of functions)	Usability/ Appropriateness recognisability
2.	Demonstration capability	What proportion of functions requiring demonstration have such capability?	A= Number of functions implemented with demonstration capability B= Total number of functions requiring demonstration capability	
3.	Completeness of user documentation and/or help facility	What proportion of functions are correctly described in the	A= Number of functions described correctly B= Total of number of functions Implemented	Usability/ Learnability

		user documentation and/or help facility?		
4.	Operational consistency	How consistently can similar operations be carried out ?	A = number of operations that behave inconsistently B= total number of operations that behave similarly	Usability/ Operability
5.	Message clarity	How easily can messages from a system be understood ?	A = number of messages that are understood easily B = total number of implemented messages	
6.	Customizing possibility	How many functions and operational procedures can a user customize for his convenience?	A=Number of implemented functions which can be customised during operation B=Number of functions requiring the customization capability	
7.	Input validity checking	What proportion of input items provide checking for valid data.	A = Number of input items checked for valid data B = Number of input items which need checking for valid data	Usability/ User error protection
8.	Avoidance of incorrect operation	How many functions have incorrect operation avoidance capability.	A = number of functions implemented to avoid critical or serious malfunctions being caused by incorrect operation B = total number of incorrect operation patterns	
9.	Appearance customizability of user interface	What proportion of user interface elements can be customised in appearance.	A=Number of types of interface elements that can be customised. B=Total number of types of interface Elements	Usability/ User interface aesthetics measures
10.	Physical accessibility	What proportion of functions can a user with a physical handicap access	A = number of functions accessible by the disabled person. B = total number of functions implemented	Usability/ Accessibility measures
11.	Access	How controllable	A= Number of detected	Security/

	controllability	is the accesses to the system?	different types of illegal operations B= Number of types of illegal operations in the specification	Confidentiality
12.	Data encryption	How correctly is the encryption/decryption of data items implemented as stated in the requirement spec.	A = number of data items correctly encrypted/decrypted B = number of data items to be required encryption/decryption	
13.	Data corruption prevention	To what extent can the data corruption be prevented?	A = number of data corruption instances actually occurring B = number of accesses where data damage or breakage is expected to occur.	Security/ Integrity
14.	Utilization of digital signature	What proportion of events requiring non-repudiation are processed using digital signature?	A = number of events processed using digital signature B = number of events requiring nonrepudiation property.	Security/ Non-repudiation
15.	Access auditability	How complete is the audit trail concerning the user access to the system and data?	A = number of accesses to system and data recorded in the system log B = number of accesses actually occurred	Security/ Accountability
16.	Authentication methods	How well does the system authenticate the identity of a subject or resource?	A = number of provided authentication methods (e.g., ID/password or IC card)	Security/ Authenticity

Results of U&S metrics descriptions analysis gave us possibility to set up variants of their interaction (table 4).

If we compare data from table 2 and 4 we can see, that sets of variants of interaction of U&S subcharacteristics and their metrics do not identical, but very similar. Some interactions were changed in the subcharacteristics context. In table 4 such changes were marked be the grey background. Such result is obvious, because U&S metrics interact with subcharacteristics

Table 4. Variants of interaction metrics of U&S subcharacteristics.

Usability metrics (sub-subcharacteristics)/ Security metrics(sub-subcharacteristics)		2.1		2.2	2.3	2.4	2.5
		Access controllability	Data encryption	Data corruption prevention	Utilization of digital signature	Access auditability	Authentication methods
1.1	Description completeness	↑↑/↓↓	?	?	?	?	?
	Demonstration capability	↑↑/↓↓	?	?	?	?	?
1.2	Completeness of user documentation and/or help facility	↑↓	-	-	-	-	-
1.3	Operational consistency	↑↑/↓↓	?	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓
	Message clarity	↑↑/↓↓	?	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓
	Customizing possibility	↑↑/↓↓	?	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓
1.4	Input validity checking	↑↑/↓↓	?	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓
	Avoidance of incorrect operation	↑↑/↓↓	?	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓	↑↑/↓↓
1.5	Appearance customizability of user interface	↑↑/↓↓	?	?	?	?	?
1.6	Physical accessibility	↑↓	?	↑↓	↑↓	↑↓	↑↓

1. Usability subcharacteristics:
   - 1.1 Appropriateness recognizability
   - 1.2 Learnability
   - 1.3 Operability
   - 1.4 User error protection
   - 1.5 User interface aesthetics
   - 1.6 Accessibility

2. Security subcharacteristics
   - 2.1 Confidentiality
   - 2.2 Integrity
   - 2.3 Non-repudiation
   - 2.4 Accountability
   - 2.5 Authenticity

.

3 Case Study

We will represent simple example of U&S interaction. First of all, worth noting, that metrics U&S equal to subsubcharacteristics (i.e. U&S subcharacteristics of second level). In this case, with usage of calculated significances, from U&S metrics, in author's opinion, it is possible to do quantitative analysis of U&S interaction. We will do such analysis for separate subcharacteristics of U&S characteristics. For example, we will consider interaction of Operability and Confidentiality subcharacteristics on basis of such interaction with metrics. For that see table. 3, which includes the description of metrics and required primitives for calculation. Object of our research will be web-site of Banking University (http://ubs.edu.ua/en/), which is on the stage of the development. We will calculate metrics of significances for web-site before making changes in this web-site (i.e. before testing). Results of calculation represented in table. 5.

Table 5. Metrics significances.

Subcharacteristics/metrics		1	2
Operability	Operational consistency	0,3	0,1
	Message clarity	0,8	1
	Customizing possibility	0,6	0,8
Confidentiality	Access controllability	0,6	0,8

1. Metrics significances before make changes (i.e. before testing);
2. Metrics significances after make changes.

For calculation of single significance for Operability subcharacteristic use additive convolution, in which weighting coefficients for significances of metrics will be equal. In result of calculation, we give following significances:

- before making changes
  $Operability_{before}$ = 0,3*0,33+0,8*0,33+0,6*0,33=0,099+0,264+0,198=0,561;
- after making changes
  $Operability_{after}$ = 0,1*0,33+1*0,33+0,8*0,33=0,033+0,33+0,264=0,627.

Further, we will compare received significances for Operability and Confidentiality subcharacteristics:

- before making changes Operability= 0,561, a Confidentiality=0,6;
- after making changes Operability= 0,627, a Confidentiality=0,8.

In result, we received significances for Operability and Confidentiality subcharacteristics. Such significances increased after making changes in web-site in comparison with before making changes. For Operability the difference equals 0,066 and for Confidentiality - 0,2. Thus, we have confirmation of our supposition about interaction of Operability and Confidentiality characteristics, when increase of level of one subcharacteristic incurring to increase in the level of other subcharacteristic (table 2).

4 Conclusions

We have considered two basic aspects of U&S interaction: usable security and secure usability. Differences in such aspects were analyzed by use of practical examples.

This work includes results of analysis of U&S interaction on the level of subcharacteristics and metrics. Results of such research give possibility to define the set of variants of the interaction of U&S subcharacteristics and metrics. Such variants of interaction of subcharacteristics and metrics are not identical, but are very similar.

In future authors are planning to make complete quantitative analysis of interaction of U&S subcharacteristics on the base of calculated metrics values. Authors suppose, that such analysis must confirm that variants of interaction of U&S subcharacteristics assessment will be correct. Also we plan to analyze interaction between U&S characteristics of information systems and another once, for example, safety.

Practical results of such assessment are improving of requirements foundation for U&S and other characteristics and correcting of design decisions.

References

1. ISO/IEC 25010: Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models, ISO/IEC JTC1/SC7/WG6, (2011)
2. Oleksandr Gordieiev. Evolution of software Quality Models in Context of the Standard ISO 25010. In. proc. Dependability on Complex Systems DepCoS – RELCOMEX (DepCOS), June 30 – July 4, Brunow, Poland. – pp. 223-233 (2014)
3. C. Shoba Bindu. Secure Usable Authentication Using Strong Pass text Passwords. Computer Network and Information Security, Vol. 3, 2015, pp. 57-64 (2015)
4. Suliman A. Alsuhibany. A benchmark for designing usable and secure text-based captchas. International Journal of Network Security & Its Applications (IJNSA), Vol. 8, No.4, pp. 41-54 (2016)
5. Julie Thorpe, Paul C. van Oorschot. Graphical Dictionaries and the Memorable Space of Graphical Passwords. In. proc. of the 13th USENIX Security Symposium, August 9-13, San Diego, CA, USA, pp. 10-26 (2004)
6. Khalid T. Al-Sarayreh, Lina A. Hasan, Khaled Almakadmeh. A Trade-Off Model of Software Requirements for Balancing Between Security and Usability Issues. International Review on Computers and Software, Vol.10(12), pp. 1157-1168 (2016)
7. Evaluating the accessibility, usability and security of Hospitals websites: An exploratory study. In proc. International conference on Cloud System and Big Data Engineering (Confluence-2017), at Noida, Uttar Pradesh, India, (https://www.researchgate.net/publication/313841977_Evaluating_the_accessibility_usability_and_security_of_Hospitals_websites_An_exploratory_study) (2017)
8. Butler Lampson. Privacy and Security Usable Security: How to Get It. Communications of the ACM, Vol. 52, no. 11, pp. 25-27 (2009)
9. Bryan D. Payne, W. Keith Edwards. A Brief Introduction to Usable Security. IEEE Internet Computing, Vol. 12, pp. 13-21 (2008)
10. Ivan Flechais, Cecilia Mascolo, M. Angela Sasse. Integrating security and usability into the requirements and design process. International Journal of Electronic Security and Digital Forensics, Vol. 1, pp. 12-26 (2007)

11. Shamal Faily, John Lyle, Ivan Fléchais, Andrew Simpson. Usability and Security by Design: A Case Study in Research and Development. Proc. of the NDSS Workshop on Usable Security, At San Diego, CA, USA, (http://eprints.bournemouth.ac.uk/22053/1/flfs15.pdf) (2015)
12. Paul DiGioia, Paul Douris. Social Navigation as a Model for Usable Security. In. proc. of Symposium On Usable Privacy and Security (SOUPS), July 6-8, Pittsburgh, PA, USA, pp. 101-108 (2005)
13. William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Michelle L. Mazurek. Usability and Security of Text Passwords on Mobile Devices. In. proc. of the CHI Conference on Human Factors in Computing Systems (CHI '16), Santa Clara, California, USA, pp. 527-539 (2016)
14. Catalin Boja, Mihai Doinea. Usability vs. Security in mobile applications. Proc. of the IE 2013 International Conference, pp.138-142 (2013)
15. Ugochi Oluwatosin Nwokedi, Beverly Amunga Onyimbo, Babak Bashari Rad. Usability and Security in User Interface Design: A Systematic Literature Review. International Journal of Information Technology and Computer Science (IJITCS), Vol. 8, pp. 72-80 (2016)
16. Oleksandr Gordieiev, Vyacheslav Kharchenko and Mario Fusani. Evolution of software quality models: usability, security and greenness issues. In proc. of the 19-th International Conference on Computers (part of CSCC 15), July 16-20, Zakynthos Island, Greece, p. 519-523 (2015)
17. ISO/IEC 25023: Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality, ISO/IEC JTC1/SC7/WG6 (2011)
18. ISO/IEC 25030: Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Quality requirements, ISO/IEC (2007)
19. Usability of security team at National institute of standards and Technology (http://csrc.nist.gov/security-usability/HTML/about.html).
20. Completely Automated Public Turing test to tell Computers and Humans Apart, CAPCHA (http://www.captcha.net/).