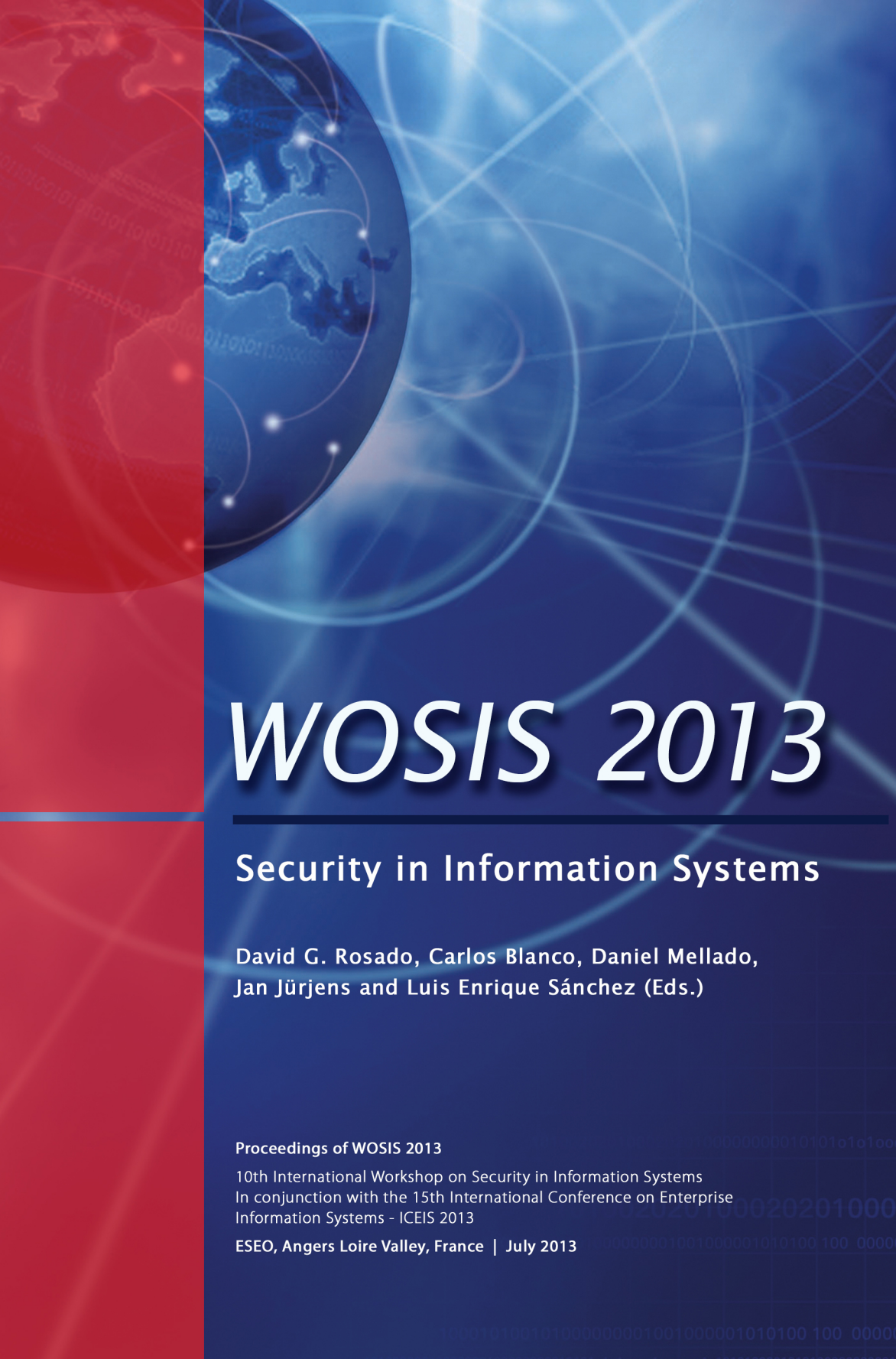

WOSIS 2013

Security in Information Systems

David G. Rosado, Carlos Blanco, Daniel Mellado,
Jan Jürjens and Luis Enrique Sánchez (Eds.)

Proceedings of WOSIS 2013

10th International Workshop on Security in Information Systems
In conjunction with the 15th International Conference on Enterprise Information Systems - ICEIS 2013

ESEO, Angers Loire Valley, France | July 2013

David G. Rosado
Carlos Blanco
Daniel Mellado
Jan Jürjens and
Luis Enrique Sánchez Crespo (Eds.)

Security in Information Systems

Proceedings of the
10th International Workshop on
Security in Information Systems
WOSIS 2013

In conjunction with ICEIS 2013
Angers, France, July 2013

SCITEPRESS
Portugal

Volume Editors

David G. Rosado
University of Castilla-la Mancha
Spain

Carlos Blanco
University of Cantabria
Spain

Daniel Mellado
Spanish Tax Agency & GSyA Research Group
Spain

Jan Jürjens
TU Dortmund & Fraunhofer ISST
Germany

and

Luis Enrique Sánchez Crespo
Sicaman Nuevas Tecnologias
Spain

10th International Workshop on
Security in Information Systems
Angers, France, July 2013

Printed in Portugal

ISBN: 978-989-8565-64-8
Depósito Legal: 360516/13

Foreword

The Tenth International Workshop on Security in Information Systems – WOSIS 2013 was organized in conjunction with ICEIS 2013 in Angers, France. As in previous years, this workshop is primarily focused on high quality and innovative research papers from different fields related to the most recent developments in Security in Information Systems. In this edition, the workshop has incorporated new topics related to security in Cloud computing and Mobile Computing.

Traditionally the best papers are published in a reputable journal dealing with WOSIS topics. This year, authors will have the opportunity to have their work selected for publication in an extended version in the well recognized ISI ranked Publication Journal such as The Computer Journal. We especially want to thank Professor Fionn Murtagh for his outstanding support throughout the whole process in publishing the best WOSIS 2013 papers in The Computer Journal.

Papers presenting the most recent theoretical, and practical works in security for Information Systems were received, a total of 19 submissions. All the submissions were reviewed by at least two program committee members. Finally, 8 papers have been accepted and 2 short papers will also have the chance to be presented during the sessions due to the excellent quality of the research.

We would like to thank all the authors who took the time to submit papers to WOSIS, even though they were not finally accepted. We would also to express our gratitude for the excellent work done by the Program Committee and the members of the Organisation Committee.

The publication of the best papers in the prestigious journal of The Computer Journal, along with the presence of a renowned Program Committee, will contribute to the success of this 10th edition of WOSIS.

July 2013,

David G. Rosado
University of Castilla-la Mancha, Spain

Carlos Blanco
University of Cantabria, Spain

Daniel Mellado
Spanish Tax Agency & GSyA Research Group, Spain

Jan Jürjens
TU Dortmund & Fraunhofer ISST, Germany

Luis Enrique Sánchez Crespo
Sicaman Nuevas Tecnologias, Spain

Workshop Chair

David G. Rosado
University of Castilla-la Mancha
Spain

Program Chairs

Carlos Blanco
University of Cantabria
Spain

Daniel Mellado
Spanish Tax Agency & GSyA Research Group
Spain

and

Jan Jürjens
TU Dortmund & Fraunhofer ISST
Germany

Publicity Chair

Luis Enrique Sánchez Crespo
Sicaman Nuevas Tecnologias
Spain

Program Committee

Andreas Bauer, National ICT Australia, Australia
Carlos Blanco, University of Cantabria, Spain
Kevin Butler, University of Oregon, U.S.A.
Pino Caballero-Gil, Universidad de La Laguna, Spain
Csilla Farkas, University of South Carolina, U.S.A.
Eduardo B. Fernandez, Florida Atlantic University, U.S.A.
Maria Carmen Fernández, University of Málaga, Spain
Eduardo Fernández-medina, University of Castilla-La Mancha, Spain
Paolo Giorgini, University of Trento, Italy

Table of Contents

Full Papers

Short Papers

Is Usability an Obstacle for Information Systems Security?

Laura Zapata[1], Ana M[a] Moreno[1] and Eduardo Fernandez-Medina[2]

[1]Faculty of Informatics, Technical University of Madrid, Campus de Montegancedo s/n, 28660 Boadilla del Monte, Madrid, Spain
[2]Department of Information Technologies and Systems, University of Castilla-La Mancha, Paseo de la Universidad 4, 13071 Ciudad Real, Spain
lm.zapata@alumnos.upm.es, ammoreno@fi.upm.es
Eduardo.FdezMedina@uclm.es

Abstract. Keeping information systems secure is costly. Organizations allocate financial and human resources in order to prevent security incidents having an impact on software applications. There is evidence that information systems security has in some cases been affected by human errors that might be caused by a poor usability design. There is clearly a link between security and usability. To clarify this, we have conducted a systematic mapping study of the literature produced over the last decade. We identified five relationship types: inverse, direct, relative, one-way inverse, and no-relationship. Most authors agree that there is an inverse relationship between security and usability, which means that increasing usability leads to a decrease in security issues in a product and vice versa. However, this is not a unanimous finding, and this study unveils a number of open questions, like application domain dependency and the need to explore lower level relationships between attribute sub-characteristics.

1 Introduction

The development of secure information systems has become critical in the last decade. The use of electronic transactions over the Internet and other networks, and the storage of an ever-increasing amount of sensitive data, is among the main factors behind this development [1].

Therefore, keeping information systems secure is by no means a simple and inexpensive task, as discussed by the Australian Governments Department of Defence [2]. Cyber security incidents can be costly, consuming financial and human resources. Examples of impacts are: service unavailability and loss of productivity, damage to the reputation of and customers confidence in the targeted organization, lost or stolen information, loss of privacy, etc.

The Microsoft Security TechCenter [3] reported a similar study, adding, however, more detailed information about costs. They consider direct and indirect costs, such as costs due to the loss of competitive edge as a result of the release of proprietary or sensitive information, legal costs, labour costs on the analysis of breaches, software reinstallation, and data recovery, costs of system downtime (for example, lost employee productivity, lost sales, replacement of hardware, software and so on).

On the other hand, Braz et al. [4] pointed out that secure systems also need to be usable. Usability is, however, wrongly added on at the end of the life cycle development process because of the mistaken belief that security is related to the software system functionality and can be designed independently of usability which relates only to the UI component.

Mechanisms for ensuring security in information systems, such as authentication, sophisticated encryption algorithms and so on are only effective when they are configured and used correctly. As a result, security experts have identified users as being the weakest link in the security chain [1].

This is when we instinctively realize that there is a link between security and usability, and system users are the nexus between the two. We might even venture to say that usability goes hand in hand with security in the context of secure information systems.

The literature is replete with major debates concerning the relationship between security and usability. For instance, Cranor and Garfinkel [5] refer to e-banking systems and some secure implementations that use the two-factor authentication method. This method consists of a user-password and an automatically generated password generally sent to a mobile device for user authentication. This clearly detracts from system usability but is, at the same time, necessary in order to establish a level of security. As the authors state, "At first glance, the source of conflict might appear obvious: security usually aims to make operations harder to do, while usability aims to make operations easier. However, it′s more precise to say that security restricts access to operations that have undesirable results, whereas usability improves access to operations that have desirable results."

From a software engineering (SE) point of view, security and usability are two independent quality factors that are specified in quality standards [6],[7],[8].

The most recent software quality standard, ISO/IEC25010 also called SQuaRE [6], defines security as "the degree of protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or system are not denied access to them". On the other hand, usability is defined as "the extent to which a product can be used by specific users to achieve specific goals with effectiveness, efficiency and satisfaction in a specified context of use". Additionally, the standards provide a set of subfactors for each of these quality attributes. The subfactors specified for security include confidentiality, integrity, non-repudiation, accountability, authenticity and security compliance, whereas, according to this standard, usability subfactors are effectiveness, efficiency and satisfaction.

Even though a thorough reading of the definitions of security and usability suggest that there is a relationship, the detailed link between the two concepts is today an open issue in the SE field. In this context, and bearing in mind that users are a key factor in secure systems, we believe that it would be important to find out of the details of the relationship between security and usability.

As far as we know, no other literature review has addressed this issue. On this ground, we conducted a systematic mapping study designed to summarize, analyse and understand what authors have been researching with respect to the relationship between security and usability over the last decade.

Our literature review focuses on security and usability as high-level quality factors. This is the prelude to more thorough-going research addressing the relationship between the characteristics and sub-characteristics of each of these two attributes.

To do this, the remainder of the paper is structured as follows. Section 2 outlines the research method that we have followed to perform the systematic mapping study. Section 3 reports the results, and Section 4 discusses our conclusions.

2 Research Method and Procedure

This section presents the process enacted to conduct our systematic mapping study of the literature related to security and usability. The guidelines provided by Petersen et al. [9] were used to build this systematic map.

2.1 Research Question

As stated above, software quality models establish security and usability as quality factors. Accordingly, we formulated the following research question:

RQ. 1. What type of relationship is there between security and usability?

This question intends to clarify the relationship between security and usability factors globally. Once we have the answer to this question, we will extend the mapping study to the characteristics and subcharacteristics of each factor.

2.2 Search Strategy

The search was run on several well-known databases, such as IEEE Xplore, ACM Digital Library and Inspec, as well as some individual journals and papers.

The publication year was set between 2002 and 2012 to limit the results to documents published within the last 10 years. Then, the titles and the abstracts of the identified articles were checked against set eligibility and relevance criteria (this criterion is explained in Section 2.3).

The literature was reviewed by a second researcher, and overlapping papers were removed.

2.3 Data Retrieval

Search strings were devised in order to collect information that can be used to answer the research question. The search strings were designed as follows:

X was composed of synonyms of or words possibly related to security in computer science, each linked by the "OR" operator.

X: Security OR secure systems OR critical systems OR critical software OR security software constraints OR security software permissions

Y was composed of synonyms of or words possibly related to usability in computer science, using each linked by the "OR" operator.

Y: Usability OR operability OR user-centred design OR UCD OR human-computer interaction OR HCI OR user interface OR UI OR ergonomics

Finally, the "AND" operator was added between X and Y to retrieve relevant literature related to security and usability (or respective synonyms) from the above data sources. Search string matching was confined to terms in the title and abstract of each publication.

2.4 Inclusion Process

The query strings devised in Section 2.3 were matched with the titles and abstracts of publications published in the last decade (2002-2012). As a result, the search process returned 120 papers for the three data sources. We read the abstract and introduction of these papers and discarded 55 papers as being irrelevant. The other 65 were retained as relevant for the research. From the resulting 65 papers, five were duplicate publications, that is, multiple data sources returned the same papers. These duplicates were discarded, leaving 60 papers. Two papers were unavailable from the electronic data sources, leaving 58 available full-text papers. We located another 17 papers in other sources, making a total of 75 papers. Of these, 33 were considered irrelevant and 42 papers were selected as being possibly useful for the research.

Finally, these 42 papers where analysed by reading the entire content in order to decide whether they were of any use for answering the research question. As a result, 25 papers were considered irrelevant, and only 17 papers were found directly related to security and usability.

3 Results

This section reports the results from the analysis of the seventeen papers detailed in the Appendix. First, we identify the different types of relationships identified by authors. Next, we classify the papers into research categories. Finally, we discuss the answers to the stated research question.

3.1 Taxonomy of Relationship Type

As already mentioned, the papers are detailed in the Appendix. From these papers, we established a taxonomy for the different relationships identified by the authors. These relationships are listed and explained below.

Inverse Relationship. Increasing or decreasing usability has the inverse or reciprocal effect on security and vice versa.

Direct Relationship. Increasing or decreasing usability has the same effect on occur in security, and vice versa.

No Relationship. The two factors are unrelated, so increasing or decreasing usability has no effect on security and vice versa.

One-way Inverse Relationship. There is an inverse relationship between the two factors, provided that the order is not changed.

Relative or Dependent Relationship. The relationship depends on some characteristic and could be direct in some cases and inverse in others.

Another point that researchers made is that the increases or decreases are not necessarily proportional. For example, increasing usability by 20% does not necessarily mean that security will decrease by the same percentage.

Fig. 1 summarizes the findings by author and type of relationship.

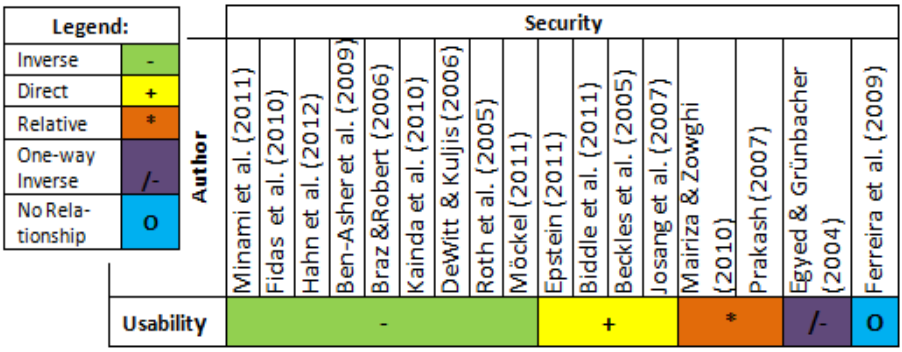

Fig. 1. Authors grouped by the type of relationship agreed.

3.2 Papers Grouped by Research Category

We grouped papers according to the classification scheme proposed by Wieringa et al. [10]. The short description of each category follows.

Evaluation research is a technique or a solution implemented and evaluated in practice. In a *validation research*, techniques are novel, but still have not been implemented in practice, however, it probably tested in a laboratory environment. In a *solution proposal*, a solution for a problem is proposed. In a *philosophical paper*, the field is structured in the form of a taxonomy, outlining a new way of looking at existing things. In an *experience paper*, the personal experience of the author on what and how something happened in practice is reported. In an *opinion paper*, the personal opinion on a particular matter is expressed.

Papers were grouped as follows: six were classed as solution proposals, five, as evaluation research, and the experience paper, validation research and opinion paper categories each contained two papers. In the next section (3.3) are explained the papers and the research category assigned.

3.3 Relationships Grouped by Authors and Assignation of Research Category

In this section, we detail the different types of relationships between security and usability identified by the reviewed authors, and the type of research category assigned to the publication.

Inverse Relationship. Fig. 1 shows that over half of the authors (nine out of seventeen) identified an inverse relationship between security and usability and vice versa. The reasons follow.

Minami et al. (2011). This paper reports evaluation research addressing the trade-off between usability and security in the context of medical systems. The authors were tasked with adding an access control and encryption method to an existing system in order to protect patient security and privacy. They gathered feedback from health professionals in order to strike a balance between strict protection and usability.

Finally, they concluded that security compromises usability, but a good balance could be achieved. Their results are valuable for our research because they used a real system tested in a real environment, and this research used other sub-factors, such as privacy and identification, which other papers often do not cover.

Fidas et al. (2010). Based on their experience, the authors argue that system designers face contradicting requirements. On one side, stakeholders are willing to sacrifice user convenience in order to achieve system security, whereas, on the other, users are interested in system usability.

The argument suggests an inverse relationship, although the authors provide no evidence. The solution that they propose is a user-centric approach to the design of a secure and usable system. This does not provide a direct answer to our research question. However, their experience is considered to be relevant for our research.

Hahn et al. (2012). This is a solution proposal paper analysing the security of many popular cloud services, such as CloudMe, Dropbox, HiDrive, etc. They analysed their vulnerabilities and listed possible attacks in an attempt to solve the discovered problems. In their analysis, they found that providers omitted email verification during registration, which is a security pitfall designed to avoid system usability problems.

From their analysis we can infer that increasing usability will decrease security and vice versa.

Ben-Asher et al. (2009). This is a validation research paper reporting the construction of a controlled research environment that they called "microworld" to quantitatively evaluate and model the acceptability of security features as a function of the usability cost of their use, efficiency and threat severity. Their study is based on the behaviour of users overriding or ignoring security features to facilitate system use. This includes an alert system that warns about possible attacks, which, if not prevented, can cause losses of monetary earnings. Using the system they were able to manipulate the usability costs of using a security feature.

Their results showed that the percentage of usage was lower at a high security level, and the percentage of usage was higher at a low security level. This suggests that there is an inverse relationship between factors tested in a laboratory experiment.

Braz and Robert (2006). This is an evaluation research paper, developing a comparative analysis of different authentication methods, such as passwords, PIN, proximity card, multifunctional card, public key, finger print and so on, and the perception of security that the user has. Results from their comparative analysis showed that methods that scored high on security were rated as having a significant level of usability issues. This applies to the listed authentication methods, including multifunctional card, public key, and Kerberos and retina/iris techniques, which have a significant impact on the usability, and especially to retina analysis, because it requires more user cooperation. On the other hand, the authentication methods that scored low on security were rated as having a low

level of usability issues. This applies to methods, such as passwords, PIN, and especially to voice, because it changes over the time, thereby decreasing security.

In other words, more security implies less usability, and less security implies more usability. They demonstrated an inverse relationship.

Kainda et al. (2010). This is a solution proposal enacting a security-usability analysis process based on a threat model. The authors highlight a difference between standard security threat models and the HCISec (HCI over information security systems) model, because malicious attackers may or may not be legitimate users in standard models, whereas HCISec focuses on legitimate user mistakes that may compromise the system. Legitimate users make mistakes that breach system security because threat scenarios are more usable than secure scenarios. The idea is to make secure scenarios more usable to reduce the risk of users making mistakes.

We infer from the view that the authors take that the relationship between factors is inverse.

DeWitt and Kuljis (2006). This is an evaluation research paper conducting a usability study on Polaris, which was built to make the Windows operating system safer from viruses and malicious code, but highly usable as well as secure. The study used a laboratory test during which users were asked to perform tasks that included the use of security. They measured learnability and usability based on standard ISO 9241-11, which defines usability as comprising effectiveness, efficiency, and satisfaction. With respect to security, they include tasks such as browsing an Internet banking website, checking emails and following hyperlinks to try out attached files.

They found that participants were willing to compromise security. They reasoned this behaviour by declaring that the speed and ease with which tasks were completed is more important than the protection of their files. This means that people favour ease of use over security.

Roth et al. (2005). This is an evaluation research paper conducting an experiment where security mechanisms were applied to protect mails sent by non-commercial users in order to find the correct trade-off between usability and security. The authors researched what the optimum trade-off should be and how security benets can be maximized with minimum damage to usability. In the case of usability, they improved the user interface by decreasing the number of interactions, and letting users handle concepts with which they were familiar, like, for example, "mail" rather than "keys". They aimed to provide a familiar context and mental model representation. In the case of security, they tried to protect the email communication from external attack and assure the data integrity.

This experiment was conducted on a particular security field, known as Attack/Harm Detection and Integrity, where the user interacts as little as possible with the issues related to security. Although this is a particular case at the subfactor level, it is a good result as far as we are concerned because few researchers have considered these security issues.

Möckel (2011). This is a solution proposal paper aiming to build an evaluation framework to align usability and security in the context of e-banking systems. We are primarily concerned with one of its research questions, namely, What is the relationship between security criteria influencing mitigation quality and usability criteria?

Möckel intimates that the relation is inverse, stating that "Most works have focused on the balance between security and usability in regard to authentication methods, often in a comparative fashion or on individual solutions. Author Murdoch discusses the problem of 'usability optimization' with a negative effect on overall system security..." Unfortunately, this research is incomplete and, consequently, we class it as an opinion paper.

Direct Relationship. Four out of the seventeen authors identified a direct relationship between security and usability and vice versa on the following grounds.

Epstein (2011). This is an experience paper establishing that it is possible to align usability and security as part of the software development cycle and not as an add-on at the end.

We interpret this as meaning that there is direct relationship between the two factors: "On occasions, security and usability are perceived as being at odds... However, this is a false dichotomy —usability also requires preventing inappropriate actions..."

Biddle et al. (2011). This is an opinion paper expressing the viewpoint that usability and security are directly related because when one is negatively affected the other will be negatively affected as well: "Usability and security are not simply inversely related, most especially because faults in one lead to faults in the other..." The authors based their opinion on their experience.

Beckles et al. (2005). This is a solution proposal paper describing two proposals to improve grid security usability.

Grid security is based on public key infrastructure (PKI), but PKI implementations have unfortunately suffered, from serious usability issues in terms of end-user acquisition and management of credentials. The specific usability issues that they found were credential acquisition, configuration complexity, mobility, user management of credentials and revocation. The approach of the first solution, named PKIBoot, is for everything to be automatically configured via user-password authentication, i.e., the client has nothing to do with settings. According to the second solution, named GridLogon, users log in for a service to access their entire security configuration.

Regarding the relationship between grid usability and security their results suggest that improvements in usability (in the area of credential management) are required if the security of these environments is to be maintained.

Josang et al. (2007). This is a solution proposal paper reporting a set of security usability vulnerabilities that can be used to assess the risk to secure systems. The solution is designed at the usability and security factor level, but the example only shows how to apply the solution at the level of one subfactor, namely, authentication for web security solutions.

The authors analyse whether upgrading usability improves security. This proposal would benefit from evaluation in practice, but the examples and the way in which the authors illustrated their solution is quite suitable for our purpose.

Relative Relationship

Mairiza and Zowghi (2010). This is a solution proposal paper cataloguing conflicts between non-functional requirements (NFR) like accuracy, usability, availability, reliability, security, etc. The conflicts were categorized as absolute conflict, relative conflict

and never conflict. Their results establish that conflict between usability and security (and vice versa) is relative, because they conflicted sometimes but not always.

Prakash (2007). This is a validation research paper reporting two studies of vulnerabilities at the user level. The first study was conducted on a group of computer science graduate students and some faculty (non-regular users). It examined the vulnerability of users to man-in-the-middle attacks on SSH. The second study analysed over 700 bank web sites for a range of vulnerabilities that resulted from poor website design decisions from a security perspective.

For the first experiment, the results indicate a direct relationship: there are widespread security problems at the end-user level in systems that attempt to deploy security protocols to secure user interactions. Advanced users bypassed the SSH security warning to log on to the server, perceiving it as an obstacle because SSH does not indicate what to do to solve the problem save contacting the administrator. This means that usability was not good enough causing security problems. From this we infer that poor usability compromises security. For the second experiment, results show an inverse relationship: setting the credential inputs on an insecure page (even when the data were sent to the server in a secure form) in order to increase the usability caused a security problem. From this we infer that good usability compromises security.

One-way Inverse Relationship

Egyed and Grünbacher (2004). This is a solution proposal paper consolidating a matrix of potential conflicts and cooperation between quality attributes from a wide range of literature and ISO 9126, such as functionality, efficiency, usability, accuracy, security and so on. This model takes into account that attributes might be indifferent to one another, cooperative or conflicting.

They found that usability is indifferent with respect to security. Inversely, however, security enters into conflict with usability. In other words, improving usability does not affect system security (there is no relationship). In the other case, however, security is inversely related to usability, because, if it increases, system usability will decrease.

No Relationship

Ferreira et al. (2009). This is an evaluation research paper consolidating a model of patterns to align usability and security. Factor patterns, such as explicit user audit, complete delete, email-based identification and authentication and so on (previously created by Garfinkel et al.). The authors validate these patterns in an experiment with computer experts, who managed to apply 61.67% of these patterns in software, concluding that they are a useful guide for developers.

These authors establish that there is no conflict between security and usability, stating that "Some authors argue that it can be complicated to build systems with both security and usability, but the reality is that there is no real conflict between these two properties". Following these guidelines, they were able to build secure software with a trade-off and without conflicts between security and usability.

3.4 Discussion

Fig. 2 shows the five types of relationship between security and usability on the horizontal axis, whereas the six research categories appear on the vertical axis.

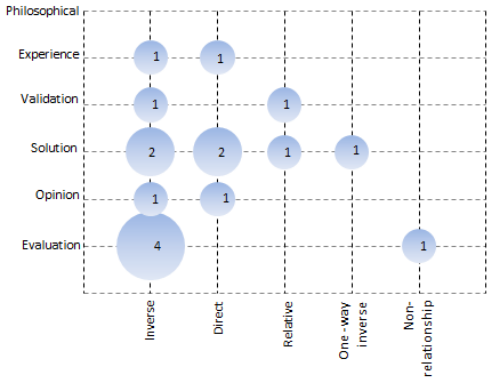

Fig. 2. Distribution of papers per category and relationship.

Clearly, most of the authors (nine) agree that security and usability are inversely related. The next group (four) agreed that there is a direct relationship. Only two authors found a relative relationship. The one-way inverse relationship and non-relationship are supported by only one author, respectively.

We consider evaluation research to be the best method for gathering evidence, because it reports solutions that have been implemented and evaluated in practice in a real environment.

As Fig. 2 shows, four out of nine papers report evaluation research that found that there was an inverse relationship, which is the relationship upon which most authors agreed.

This evaluation research was conducted in a specific setting, including access control and encryption, authentication methods, attack detection in an operating system, and attack detection over emails.

From these results, we can conclude that the inverse relationship is the most reliable response to our research question. However, we also found some evidence of contrary findings.

There is one prominent case. Prakash (2007) reports validation research showing a relative relationship between security and usability. He found a direct relationship in one experiment and an inverse relationship in another experiment. The first experiment involved computer science students using Secure Shell (SSH), which is a cryptographic network protocol. The second experiment was about vulnerabilities produced by poor user interface decisions.

Comparing these two results, the relationship appears in our opinion to be relative, that is, it depends on the subfactor of security and/or usability to be measured. Therefore, more research is required at the subfactor level, as it is far from straightforward to define a relationship from a global perspective between security and usability without analysing each of their subfactors.

Another point is that the relationship probably depends of the application type. However, more research is needed to formally assure this issue.

There is not much evidence to defend the other relationships (direct, one-way inverse and no relationship). For example, one paper that found a direct relationship is based on experience and the other exemplifies the author′s opinion. This means that there is no real quantified evidence. Finally, the other two are solution proposals which required evaluation in a real environment.

Only one author proposes a one-way inverse relationship. He claims that security changes alter usability, but the opposite does not apply. From this we infer that this relationship is probably a particular case of a relative relationship.

One paper suggests that security and usability are not related. In this case, the authors claim that there is no conflict between these factors. However, we think that their solution targets the alignment of these two factors. In this case, striking a balance between security and usability in order to improve these two factors does not necessarily mean that there is no conflict.

A significant number of papers examine the trade-off between security and usability to strike the correct balance between the two factors. This balance is important, because users are unlikely to use a 100% secure system if this significantly compromises usability, for example, by 50%.

Other authors claim that there is a relationship between security and usability, although they do not provide explicit details about the connections. This is the case of Cranor and Garfinkel [5], who have identified users as the weakest link in the security chain. This is a clear sign of there being a relationship, because it is the users that operate the systems and, at the same time, handle sensitive information like passwords, bank information, and so forth.

3.5 Threats to Validity

Until we find other systematic reviews focusing on the taxonomy of the relationship between security and usability, we will not be able to validate our study externally. Regarding internal validity, all three authors were involved in this systematic mapping study. We discussed and agreed on the procedure and considered activities to counteract the effect of researcher bias. On the other hand, we used general terms and placed no constraints on the search strings in order to achieve better coverage as well as high accuracy. We selected three of the most important electronic data sources to which we had access, and added other external sources. The chosen time-frame was intended to include the last decade of research.

During the exclusion process, we were particularly careful not to discard any potentially interesting paper. For this reason, we also included papers whose abstract or title was not completely clear with respect to our research question for further reading. It was also rather difficult to distinguish the research focus of some papers. So, even though we agree on the result of this process, replicating authors might categorize the studies differently.

The papers do not directly answer the research question, and we had to identify the response by analysing and inferring what authors had found in their research. However, we negotiated this process.

4 Conclusions

Our systematic mapping found five types of relationships between security and usability addressed by authors during the last decade. These types are: inverse, direct, relative, one-way inverse and no relationship.

The inverse relationship is the most often mentioned connection, followed by the direct, and relative relationships, where the least supported associations are one-way inverse and no relationships.

We based our results on the type of research conducted by the authors, where more weight is attached to evaluation research because results are more reliable.

A significant number of authors agreeing on an inverse relationship conducted evaluation research; however, another author who ran two different experiments found a relative relationship. Therefore, it is also necessary to analyse whether application type influences the results.

There is less evidence to support the other relationships (direct, one-way inverse and no relationship).

In sum, the literature regarding the relationship between security and usability published over the last decade is not unanimous. This point required further empirical research to study this relationship at the level of characteristics and subcharacteristics of both quality factors. This is the next step in our research.

References

1. Ben-asher, N., Meyer, J., Parmet, Y., Moeller, S., Englert, R.: An Experimental System for Studying the Tradeoff between Usability and Security. International Conference on Availability, Reliability and Security (2009)
2. Australian Government′s Department of Defence: Preparing for and Responding to Cyber Security Incidents. (2012) [Online] Available from: http://www.dsd.gov.au/publications/csocprotect/preparing_for_cyber_incidents.htm.[Accessed 5th April 2013]
3. The Microsoft Security TechCenter: Responding to IT Security Incidents. (no date) [Online] Available from: http://technet.microsoft.com/enus/library/cc875825.aspx. [Accessed 5th April 2013]
4. Braz, C., Seffah, A., M′Raihi, D.: Designing a Trade-off between Usability and Security: A Metrics Based-Model. Springer volume 4663, (2007) 114-126
5. Cranor, L., Garfinkel, S.: Security and Usability Designing Secure Systems that People Can Use. INTERNATIONAL Journal of Computers and Communications Issue 1, OReilly Media. (2005)
6. ISO/IEC, 2011, ISO/IEC 25010, Software Product Quality Requirements and Evaluation (SQuaRE) Quality Models for Software Product Quality and System Quality in use. International Standard. Switzerland
7. ISO 9126-1, 2001, Software engineering Product quality Part 1: Quality model. International Standard. Switzerland.
8. ISO 9241-11, 1998, Ergonomics of Human System Interaction - Part 11: Guidance on Usability. International Standard. Switzerland.
9. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic Mapping Studies in Software Engineering. 12th International Conference on Evaluation and Assessment in Software Engineering, (2008)

10. Wieringa, R., Maiden, N., Mead, N., Rolland, C.: Requirements Engineering Paper Classification and Evaluation Criteria: a Proposal and a Discussion. Journal of Requirements Eng, (2006)

Appendix

Literature Reviewed

-Beckles, B., Welch, V., Basney, J.: Mechanisms for increasing the usability of grid security. Int. J. Human-Computer Studies 63, (2005) 74101
-Ben-asher, N., Meyer, J., Parmet, Y., Moeller, S., Englert, R.: Security and Usability Research Using a Microworld Environment. Deutsche Telekom AG as part of the Telekom Laboratories, (2009)
-Biddle, R., Brown, J., Chiasson, S., Martin, A.: Security Dialectics and Agile Software Development. Position Paper for the 1st Software and Usable Security Aligned for Good Engineering (SAUSAGE) Workshop, (2011)
-Braz, C., Robert, JM.: Security and Usability: The Case of the User Authentication Methods. International Journal of Human-Computer Studies, (2006)
-Dewitt, A., Kuljis J.: Aligning Usability and Security: A Usability Study of Polaris. SOUPS '06 Proceedings of the second symposium on Usable privacy and security, (2006)
- Egyed, A., Grünbacher, P.: Identifying Requirements Conflicts and Cooperation: How Quality Attributes and Automated Traceability Can Help. Focus persistent software attributes, (2004)
-Epstein, J.: Integrating Security & Usability Into the Software Development Lifecycle. Position Paper for the 1st Software and Usable Security Aligned for Good Engineering (SAUSAGE) Workshop, (2011)
-Ferreira, A., Rusu, C.: Roncagliolo, S.: Usability and Security Patterns. Second International Conferences on Advances in Computer-Human Interactions, (2009)
-Fidas, C., Voyiatzis, A., Avouris, N.: When Security Meets Usability: A User-Centric Approach on a Crossroads Priority Problem. 14th Panhellenic Conference on Informatics, (2010)
-Hahn, T., Kunz, T., Scheneider, M., Sven, V., Moeller, S., Englert, R.: Vulnerabilities through Usability Pitfalls in Cloud Services: Security Problems due to Unveried Email Addresses. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, (2012)
-Josang, A., AlFayyadh, B., Grandison, T., AlZomai, M., McNamara, J.: Security Usa-bility Principles for Vulnerability Analysis and Risk Assessment, 23rd Annual Computer Se-curity Applications Conference, (2007)
-Kainda, R., Flechais, I., Roscoe, A.: Security and Usability: Analysis and Evaluation, International Conference on Availability, Reliability and Security, (2010)
-Mairiza, D., Zowghi, D.: Constructing a Catalogue of conflicts among non-functional Re-quirements, 5th International Conference, ENASE, Athens, Greece, (2010)
-Minami, M., Suzaki, K., Okumura, T.: Security considered harmful A case study of trade-off between security and usability. The 8th Annual IEEE Consumer Communications and Net-working Conference - Work in Progress (Short Papers), (2011)
-Möckel, C.: Usability and Security in EU E-Banking Systems towards an Integrated Evaluation Framework. IEEE/IPSJ International Symposium on Applications and the Internet, (2011)
-Roth, V., Straub, T., Richter, K.: Security and usability engineering with particular attention to electronic mail. International Journal of Human-Computer Studies, (2005)
-Prakash, A.: Security in Practice Security-Usability Chasm. Information Systems Security Lecture Notes in Computer Science Volume 4812, (2007) 1-9