# Rethinking Security Requirements in RE Research

Technical Report

Hanan Hibshi[1,2], Rocky Slavin[3], Jianwei Niu[3], Travis D. Breaux[2]

College of Computing[1]
King Abdul-Aziz University
Jeddah, Saudi Arabia

Institute for Software Research[2]
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
{hhibshi,breaux}@cs.cmu.edu

Department of Computer Science[3]
University of Texas at San Antonio
San Antonio, Texas, USA
{rslavin,niu}@cs.utsa.edu

***Abstract*— As information security became an increasing concern for software developers and users, requirements engineering (RE) researchers brought new insight to security requirements. Security requirements aim to address security at the early stages of system design while accommodating the complex needs of different stakeholders. Meanwhile, other research communities, such as usable privacy and security, have also examined these requirements with specialized goal to make security more usable for stakeholders from product owners, to system users and administrators. In this paper we report results from conducting a literature survey to compare security requirements research from RE Conferences with the Symposium on Usable Privacy and Security (SOUPS). We report similarities between the two research areas, such as common goals, technical definitions, research problems, and directions. Further, we clarify the differences between these two communities to understand how they can leverage each other's insights. From our analysis, we recommend new directions in security requirements research mainly to expand the meaning of security requirements in RE to reflect the technological advancements that the broader field of security is experiencing. These recommendations to encourage cross-collaboration with other communities are not limited to the security requirements area; in fact, we believe they can be generalized to other areas of RE.**

***Keywords-requirements; security; privacy; usability; literature survey***

## I. INTRODUCTION

Information security is a major concern for organizations worldwide. Routinely, different organizations report a variety of statistics regarding data breaches, IT costs, etc. that reflect the importance of security to government, businesses, and individuals. In a recent Ponemon Institute study, the average cost of data breaches per organization was estimated at $5.5 million in 2011 [74]. In 2002, the National Institute of Standards and Technology (NIST) reports the cost of $59.5 billion to the U.S. economy as a result of faulty or malfunctioned software [68].

Requirements engineering is an essential phase for software systems that can be used to address security early in development. According to Zave's definition, requirements engineering is concerned with "*constraints on software systems*" [101] and security is viewed as such a constraint on a system's behavior [31, 49]. Consequently, requirements engineering researchers argue that one goal is to develop requirements that guarantee the system does not meet the requirements of an attacker whose goal may be to compromise confidentiality, integrity or availability in the system [31, 63]. The idea of viewing the attacker as a harmful stakeholder with negative requirements was investigated further by Sindre & Opdahl when they proposed using "*Misuse cases*" to help elicit security requirements [10, 85, 86,]

The use of RE methods to improve security is an essential step towards developing a successful system [2]. Once deployed, the cost of error correction can be 10 to 200 times higher than if the error was detected during the requirements phase [7, 62]. In the case of security requirements, it becomes more expensive to improve a system's security once it's operational [2].

Because of the importance and high impact of security requirements in any system, researchers in RE have studied security requirements and suggest a variety of methods that can be used by engineers. They aim to encourage organizations towards the adoption of security requirements methods into their systems [2].

Companies still fail to implement well known security requirements. This leads us to consider "usable security," which is a collection of research efforts aimed at improving the usability and accessibility of security information and techniques. Usable security researchers approach the problem by conducting interdisciplinary research across software engineering, human computer interaction, social science and economics to understand what factors affects security decisions in systems [13]. We believe this community shares a common goal with RE security requirements research, satisfying the stakeholder's goals.

At first glance, one might mistakenly think that usable security is about designing user-friendly interfaces and conducting user studies to examine the friendliness of those interfaces. This is assumption is not completely true [13,78] as the field is looking at a wider breadth of problems that encourage "security by design." Security by design aims to incorporate system security at very early design stages [13], which is also the goal of requirements engineering.

In this paper, we report on a survey of prior work published in the IEEE Requirements Engineering Conference Series with regards to security. We also report on a parallel survey on prior work published in the

Symposium of Usable Privacy and Security (SOUPS). Our goal is to understand the historical trends and evolution in the two fields and contrast them in a way that provides suggestions for RE researchers moving forward in security. In addition to suggesting directions of future research in security requirements, we provide researchers with a systematic methodology to survey and investigate possible research in other fields that can link back to requirements engineering. Requirements engineers can take our approach and tailor it to be applied to any field of interest in order to leverage areas of innovation outside the RE community.

The remainder of this paper is organized as follows: in Section II, we motivate the link between security and requirements by returning to Jackson's World and the Machine [38]. Next, we describe our research method in Section III. In Section IV, we present our observations on security requirements research in the RE community, before we describe our survey results from the usable security community in Section V. In Section VI, we compare the literature from these two research communities. Finally, we provide suggestions and recommendations for future research in security requirements in Section VII.

## II. Security Requirements Problem Space

Before we survey security requirements, let's look at the problem from another angle: Jackson's view that consists of world phenomena, machine phenomena, and shared phenomena between the two. Shared phenomena may include a state or an event viewed by the world and the machine but only controlled by one of these domains [38]. Furthermore, Jackson defines four facets that can help shape the relationship between the world and the machine: the *modeling* of the world by the machine; the *interface* that enables the word to physically touch the machine; the *engineering* that enables the machine to take control over the behavioral aspect of the world; and the *problem* "*where the shape of the world and of the problem influences the shape of the machine and of the solution*" [38]. Framing the security requirements problem within this context is not trivial, because we may think of security in a number of ways. Since security is not a standalone problem in its own right, it can coexist in the world of other problems as we explain below.

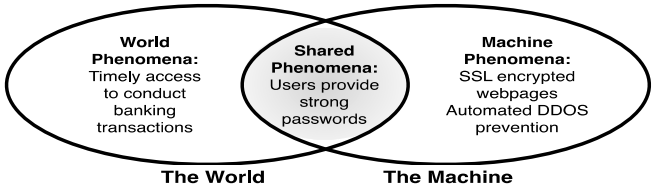


Figure 1. The World and the Machine illustrating security

When we look at the examples Jackson provides in his paper to illustrate his theory, we may infer that he assumed a *good* world and a *good* machine where everything works as *expected*. The elevator or "*lift*" that Jackson refers to as an example, was described in a setting where the input is coming from pressing the buttons of the "lift shaft" at each floor. In our world today, even this closed system of an elevator is potentially susceptible to malicious behavior that aim to misappropriate the machine. Security requirements deal with this *unexpected* situation or behavior. Nowadays, system design cannot only consider the good system that behaves normally in a good world. The buffer overflow problem is a good example of this where malicious code exceeds the size limits of the input buffer to access critical areas in the memory, which can eventually cause the program to behave unexpectedly [88].

In Figure 1, we present the World and Machine to illustrate the phenomena of security. In the world, people conduct their daily business: lifts carry people to their destinations, people coordinate their plans, and they engage in regular transactions, such as banking. In the machine, technology is designed to process information on behalf of people and these activities. Machines maintain models of the world: which floors need the lift, "who knows who" in a social network, and financial accounts. For security, shared phenomena include the various ways that users engage with the system in positive ways (e.g., call the lift, send friends photos of their latest meals, or pay bills online). However, shared phenomena also include attackers who look to repurpose the machine in ways unanticipated or undesired by other users in order to execute malicious acts: send unsolicited e-mail, steal money, and so on. Thus, while requirements engineering has focused on better understanding of the world, security researchers have been largely pre-occupied with the machine. In between these two domains, usable security researchers often target the shared phenomena as a way to make security easier to access and deploy.

## III. Methodology

Our research methodology consists of conducting two literature surveys in security requirements and usable security, before systematically comparing the results. We now discuss these steps in detail.

### A. Security requirements survey method

The survey method begins with selecting papers from the IEEE Requirements Engineering Conference Series proceedings published in the IEEE Digital Library. We restricted our search to papers published in the conference series that include the keyword "security", which yields 111 papers that fall between the years 1993 and 2012. Note that our search criteria took into account that there were two RE conferences prior to the year 2002: the IEEE International Symposium on Requirements Engineering (1993, 1995, 1997, 1999, 2001), and The International Conference on Requirements Engineering (1994, 1996, 1998, 2000). In 2002 the two conferences merged and become the IEEE International Conference on Requirements Engineering. In addition to these conferences, there was another conference in our results: the 2008 Requirements Engineering Visualization (Rev'08). Next, we refined the results by

removing workshop and poster papers to include only full research papers and short papers that are not less than 6 pages. The final result was 35 research papers.

We analyzed the resulting papers as follows: first we identified the area(s) of security that the paper addresses; examples of such areas include: privacy, access control, authentication, etc. To identify security areas, we examined the security terms that appear in the paper and how these terms were used. To make this step as accurate as possible, the first and second author analyzed the papers separately and compared results afterwards. Second, we classified each paper using the RE'13 "topics of interest" found in RE'13 call for papers [76]. Because the papers are written for the RE conference and the authors are familiar with RE research, this step was straightforward. We adhered to how the authors described their own work in their paper as opposed to using our personal judgment. The "topics of interest" that we used are as follows:

- *Requirements engineering process definition, measurement, and improvement*
- *Stake holder identification, engagement and management.*
- *Requirements elicitation, analysis, documentation, validation, and verification*
- *Requirements negotiation, prioritization, and domain ontology construction*
- *Requirements specification languages and model-driven approaches*
- *Modeling of requirements, goals, and wider system concerns*
- *Requirements management and traceability*
- *Evolution of requirements over time, product families, and variability*
- *Requirements across the entire system lifecycle*
- *Domain-specific problems, experiences, and solutions*
- *Requirements in market-driven, service-oriented, and product line environments*
- *Requirements for highly complex systems on a global scale*
- *Requirements for large-scale procurement contracts*
- *Social, cultural, global, personal, and cognitive factors in requirements engineering*
- *Industry and research collaboration, learning from practice, and technology transfer*
- *Requirements engineering education and training*
- *Tool support for requirements engineering*

### B. Survey of usable security research

We selected research papers published in the Symposium of Usable Privacy and Security (SOUPS) proceedings to survey the area of usable security. The SOUPS proceedings are published in the ACM Digital Library, and we included every publication year from 2005-2012. Similar to our RE survey, we excluded all posters and tutorials to yield 109 papers. Unlike the papers in RE, each paper in a SOUPS proceeding (except 2005) is labeled with a session name that represents the paper's primary security area. For 2005, we examined the paper titles and abstracts and then classified the papers by a relevant security area.

Since that SOUPS papers were not written for the RE audience, the act of classifying the papers by a requirements topic was not straightforward. Thus, the first and second authors examined the papers separately and classified them using the "topics of interest" listed in Section III.B. The topic of "domain-specific problems, experiences and solutions" was excluded because SOUPS papers vary less in this regard and the "stakeholder" topic was also excluded since SOUPS papers are generally user-focused. Afterwards, they met and compared their results and discussed their disagreements (if any) until they reached consensus.

To decide on the requirements classification, the researchers first met and negotiated to agree on what the analysis criteria should be. The criteria are as follows: each examiner reads the abstract of the paper, if the abstract is too general, then the body of the paper is skimmed (or fully read in some rare cases). We are interested in understanding what the paper is contributing from an RE point of view. For example if a paper describes a new way to visualize or model security guidelines, then that paper would fall into requirements modeling; alternatively, if a paper describes a survey of different users (stakeholders) of the system to collect data that helps determine appropriate user needs, then that paper is classified under requirements elicitation. We recognize the techniques used in SOUPS are not equivalent to the RE community, however, there is often overlap: notations used to model security practices and experimental methods used to survey users needs could also be used in RE. Later we will talk about the differences between papers in shared categories.

Recall, papers published in SOUPS were already labeled with a session name that represents the area of security they fall in. For papers that were published in 2005, we gave our own classification based on reading the title and abstract. Although assigned to a single session, some papers can fit into multiple sessions (judging by the session name), and we took that factor into consideration when we quantified the number of papers in each security area. However, except for SOUPS 2005, we didn't go beyond the session name in our aggregation because we want to keep the original security classification of the paper. For example, if a paper was labeled with a session name: "*privacy on social networks*", we would label this paper to fall under privacy as well as the social networks topic area.

### C. Comparison of Research

After conducting the two surveys, the authors met and compared their findings by answering the following two research questions:

**RQ$_1$**: How is security addressed in each community? What does the term *"security"* mean?

**RQ$_2$**: How does this work fit, scale, or serve requirements engineering research?

The research questions framed our analysis helped us draw findings that led to discovering new opportunities for security requirements engineering. We discuss that further in Section VI of this paper.

## IV. Security Requirements Engineering Research

We now discuss the findings from our survey of security requirements research in RE.

### A. Meaning of Security

The 35 RE papers that we analyzed dating from 1993 to 2012 continue to illustrate a change in focus in the RE community. In Figure 2, we present the number of security-related papers, which increase over time most prominently after 2006. Based on our paper classification, we found the first reference to security in Anderson and Durney's "Using Scenarios in Deficiency-driven Requirements Engineering," in which they described a process for formally specifying requirements using a deficiency-driven approach [3]. The authors used access control to model their scenario and detect incompleteness and un-safeness in order to address security. In 2007 and 2008, five of the nine security-related papers only use security as an example rather than a main topic. For example, Schneider et al. describe a notation for visualizing requirements flow and use the elicitation and validation security requirements in a very generic sense as an example [80]. On the other hand, Jeffors and Heitmeyer used a specific instance of a cryptographic device to demonstrate their algorithms for generating state invariants from requirements specification [39]. This common use of security as an example rather than a topic of research suggests there is room for more involvement with the security community.

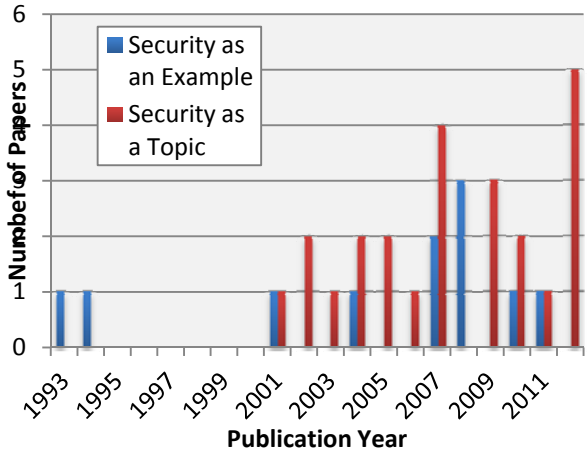


Figure 2. Comparison of papers using security as a topic and security as an example

As security becomes more established in RE, we find papers presenting frameworks and modeling languages used for security requirements. Variations on i*, a framework to model requirements as relationships among actors and goals, were introduced to address security requirements. Liu et al. expand upon i* to enable analysis of vulnerabilities and abuse [59]. Similarly, Crook et al. apply i* to model access policies by extending the framework to systematically define roles and improve the modeling of access policies [14]. Like i*, Secure Tropos is an agent-oriented framework which allows for the integration of security analysis during the development process for the sake of requirements [65]. It is based on the Tropos methodology [67] for general requirements modeling throughout the software lifecycle. Giorgini et al. further expand upon Secure Tropos by adding delegation and trust notions thus providing a way to analyze ownership, permission and delegation [28]. These papers regarding i* and Secure Tropos illustrate the early shift toward security as a topic of interest.

Figure 3 shows the representation of topics of interest in RE from 2001-2012. Areas such as requirements engineering education and training, stakeholder identification, engagement, and management, and requirements in market-driven, service-oriented, and product line environments were not represented. Security was most represented in the areas of elicitation and analysis, model-driven approaches, industry and research, and modeling. This may be due to how security can often be viewed in the RE community as a quality concern. Security is listed alongside reliability, usability, look-and-feel, extendibility and system performance as a quality requirement that must be balanced among other system concerns [55, 77]. Chung et al., for example, mention security along with accuracy and performance as a quality requirement to support change in design decisions and other non-functional requirements [12]. Further, only 25 of the 35 papers we reviewed addressed security as a main topic among 17 possible RE topics. This suggests that security is underrepresented within the RE proceedings and, because of the small sample size, there is not enough involvement for it to be covered in all topics.

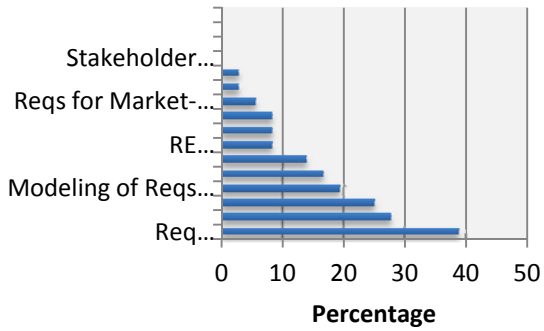


Figure 3. Distribution of topics of interest in RE proceedings

Security areas and concepts such as application security, auditing, forensics, and incident response – all notable security areas – were not represented. Instead, there tended

to be more interest in areas such as privacy, risk, compliance, and general system security. Security was most represented through privacy, which was often the subject of modeling and analysis. By modeling trust relations and attacker involvement, researchers created means for tradeoff and risk analysis [22, 59]. Similarly, Katz and Rashid defined security in terms of addressing privacy and used it as a system aspect to illustrate a framework for aspect-oriented systems for traceability [46]. Privacy was also analyzed based on social factors such as the impact by and desires of stakeholders. Antón et al. analyzed consumer perceptions on privacy in order to offer researchers and policy makers' insight into the relationship between policy and stakeholder values [4]. The need for analysis of consumer factors was also presented by Tun et al. in order to show the possibility of changes in privacy based on consumer actions or preferences [93]. The authors introduce "privacy arguments" as a means for selective disclosure requirements.

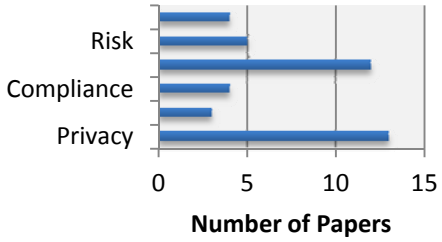


Figure 4. Distribution of security topics in RE proceedings

We categorized 12 papers as dealing with general security rather than a specific security topic such as access control or authentication. In such papers, security tended to be mentioned as a very general property such as a quality concern, which is affected by other, forces and must be balanced or satisfied [12, 39, 55]. In other cases, security is referred to in an even more general sense. For instance, Kang and Jackson refer to "general system security" and general system vulnerability as aspects of dependability [45]. Along these lines, a need for defining the role of security in requirements was also a recurring topic, which is also an important observation on the collection of papers as a whole. The state of disagreement on what role security plays in requirements was apparent by how the role of security requirements was described as both a functional and non-functional requirement depending on the authors. Toval et al. point out that while the RE community typically views security requirements as being non-functional, there is an increasing trend to integrate views from other security communities, which involve both functional and non-functional security requirements [92]. Their research concerns a personal data protection catalog, which contains both functional and non-functional security requirements. Others view security requirements as purely non-functional. For instance, Chung et al. create a framework for goal achievement which classifies security as a non-functional or quality requirement [12]. Similarly, Liu et al. implement a framework based on i* for analyzing security as a quality attribute, which is often viewed as a non-functional requirement [59].

It is also apparent that the RE community often views security requirements as goals to be satisfied as opposed to threats to be mitigated [101]. A common goal-based approach involved using security objectives as the goals and generating requirements to reach those goals [12, 14, 26]. For example, Antón et al. align requirements with privacy policy by finding privacy goals and analyzing internal system conflicts in order to construct corresponding requirements [4]. Variations on this premise involve different ways of interpreting goals. Haley et al. define some general security goals based on the qualities of confidentiality, integrity, availability and authentication [31]. These goals are used in conjunction with system assets in order to recognize possible security threats.

Rather than using security concerns as goals, another kind of goal-oriented approach used security as a secondary objective to other system obligations and goals [22, 66]. These goals are usually in the form of functional requirements. Moralı and Wieringa, for example, model stakeholder goals with obstacles for achievement. Security, in terms of confidentiality, requirements used to mitigate those goals are set in place to help fulfill the goals [64].

Based on these observations, we find that security is commonly viewed in the RE community as a non-functional requirement, a goal , an example or an aspect of another kind of requirement.

### B. *Relationship to requirements*

The majority of RE papers self-classify themselves based on the "topics of interest". We now review the most popular topics of interest in RE among our 35 security papers, shown in Figure 3.

*1) Requirements elicitation, analysis, documentation, validation, and verification*

14 of the 35 papers we reviewed fell into this category as requirements validation or analysis. Security specification validation was first mentioned by Anderson and Durney where they used general system security to illustrate an approach based on state transitions which detects and addresses deficiencies between state transitions [3]. Franqueira et al. implement backward traceability for risk mitigation to provide a means to validate risk argumentation [26].

Analysis made up the largest portion of this RE topic for security requirements. Glinz, analyzed the various uses and definitions of security as a non-functional requirement within the RE community [29]. By studying the various interpretations of requirements, including security as a non-functional requirement, Glinz created a taxonomy concentrating on system requirements, which attempts to solidify the distinctions between different types of

requirements. This taxonomy classifies security as a specific quality requirement, which "pertains to a quality concern other than the quality of meeting the functional requirements" [29]. Another good example of security analysis takes into account the assumptions made during requirements analysis, which may affect the creation of security requirements [31]. The authors argue that since the foundations of security requirements in a system are based on certain actors, which must be trusted, such as humans, the security requirements are directly related to those assumptions.

*2) Requirements specification languages and model-driven approaches*

For the second most popular topic, we found many papers that expand upon existing modeling techniques and methodologies such as the i* and Secure Tropos methodologies mentioned in the previous subsection. Similar papers model aspects of security such as risk, privacy and delegation in order to assess requirement specifications by formally modeling security concerns. For instance, Katz and Rashid present a framework, which uses linear temporal logic for proof of obligations including security of data [46]. The evaluation consists of the modeling of threats and the operations involved so that the resulting threat tree provides a means for making informed decisions by visually representing what goals must be met.

*3) Social, cultural, global, personal, and cognitive factors in requirements engineering*

The area of social, cultural, and cognitive factors was one of the top five topics of interest for RE and it is interesting because it tends to deal with external factors. All but one of the papers in this topic dealt with compliance and social regulations [4, 9, 47, 60, 71]. Interestingly, we did not find any papers that used empirical analysis to survey or understand individuals with respect to security. Instead, this topic was dominated by interest in security as an external or social factor to be integrated in terms of requirements.

While most topics include papers using security as an instance or example of another requirements matter such as non-functional requirements, requirements specification algorithms and testing [77, 39, 94], these examples show the use of security as a rising topic of interest in RE. By analyzing how security is included we get a good picture of how the RE community views security as well as what areas may be lacking in research and information.

## V. USABLE SECURITY RESEARCH

In the previous section, we analyzed the research done on security requirements in the requirements engineering conference series. In this section, we review research papers published in the Symposium on Usable Privacy and Security. When we looked the SOUPS 2013 call for papers [89], we saw some connection between that community and RE research. For example, the SOUPS community encourages concepts like: learning from practice, industry and research collaboration, new design models. Those concepts, for example, describe some of the work we see also in RE.

### A. Meaning of security

As we mentioned in Section III, we used the SOUPS session names to categories the papers. In some years, some papers were labeled as "*Soups du Jour,*" which means "*of the day*" and refers to new ideas or current trends in security topics of that publication year. We find this specific label interesting because it's a nice way that the conference encourages innovation, brings up new research areas, and keeps up with the rapidly technology trends. In Figure 5, we show the distribution of security topics for all papers from 2005 to 2012.

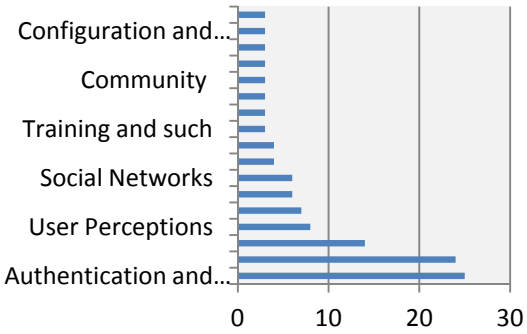


Figure 5. Distribution of security topics in SOUPS proceedings

As we can see in the numbers provided in Figure 5, SOUPS conferences covered a variety of security related topics. However, consolidating by session names was not enough for us, so to examine the topics variety further and in an attempt to understand the evolution of SOUPS topics over the years we investigated the session labels along with the paper titles in each year of proceedings. We observed that new topics come to the conference and perhaps; they get more attention until they get assigned their own session in later years. For example, in 2010, there was an increase in number of papers addressing mobile security [19, 72, 44, 36, 40, SDYB+10]. In 2012, mobile privacy and security got its own session [11, 33, 25]. Security and privacy issues related to social networks, such as Facebook, is another popular topic in SOUPS that gets more attention over the years [ 87, 23, 95, 83, 51, 41, 75]. Other examples of new security topics that we see introduced into SOUPS include: location-sharing [35, 40, 73], phishing [18, 20, 50, 58, 97 99 ], and cloud privacy issues [37].

Moreover, as technology breakthroughs continue rising in the IT world, we see some reflections of those on the SOUPS publications. In other words, researchers become more innovative by creating a diversity of ideas that apply new technology solutions to security to serve the goal of usable security. For instance, different biometric techniques had been suggested as a means of authentication. A paper

titled “Look into my Eyes! Can you guess my Password?” by De Luca et al. has introduced an eye tracking authentication technique as a secure yet usable solution that improves security in public areas [16]. This kind of innovation, expands current security topic areas, and possibly creates more areas for future research, which, in turn, expand the meaning of security.

Another interesting aspect when it comes to defining security within SOUPS is how security is defined according to users. Researchers in the usable security community try to apply different methods to elicit the meaning of security from a user point of view. By understanding what security means to a system’s stakeholder, the definition of security expands to include aspects and factors that might not be obvious in its relationship to security. To better understand the user, many SOUPS papers report studies of cognitive factors affecting users’ security decisions. Let’s take passwords as an example, when the security community thought about the password requirement problem, they thought about it in terms of increasing security by making it less “guessable”; and we see this idea reflected in the NIST recommendations for authentication [69]. However, Shay et al. have shown in their work on passwords that such traditional password requirements do not necessary improve security because there are other aspects to security such as usability [82]. This and other password-related work shows how studies of cognitive aspects can illustrate the effectiveness of security requirements in the user’s context [21, 24, 82, 98]. The focus on *usability* may be inspiring researchers to be creative and imagine different types of password requirements that are non-traditional, such as and graphical passwords [96, 100, 21]. You may need to reverse engineer the requirements from the solution, however. Requirements are satisfied by potentially many solutions. In this case, perhaps the requirement is "easy to remember" that yields so many variations, as opposed to "difficult to crack".

### *B. Relationship to requirements*

Identifying the relationship between usable security and requirements engineering may seem obvious at an abstract level. However, as we mentioned, examining each paper and trying to position it under requirements is not a straightforward task. Hence, we will highlight some of our key findings and provide examples that will illustrate them.

For the “*RE process*” category, we didn’t find any paper that matches the criteria for process.. One reason for that is the nature of the usable security field. The field aims to improve security practices by improving usability. Researchers propose design improvement ideas, but we were unable to identify research on the requirements process. Another reason could be that these papers are written from the solution space, where a solution is envisioned, as opposed to the problem space, where requirements are the main focus.

Other RE categories that we couldn’t find in SOUPS papers to fit below were: evolution of requirements over time, products families and variability, requirements across the entire system lifecycle, requirements for highly-complex systems on a large scale, and requirements for large-scale procurement contracts. Similar to the RE process category, those areas are specific and very unique to requirements engineering research.

According to Nuseibeh and Easterbrook [70], identifying stakeholders, their goals and needs is, by definition, a major component of the RE process [70]. They also state that stakeholders of a system are so diverse because they vary based on number of factors such as their goals, tasks, roles, etc. Based on this definition, we concluded that all the 109 papers published in SOUPS falls under the stakeholder identification category of RE. The usable security research is about engaging the different stakeholders of the systems to understand how they use the system by analyzing, their needs, goals, tasks, roles, as well as other factors outside the system’s context that might affect their interaction with the system [13]. Let’s look at location sharing for example: a paper by Patil et al. [73] tries to collect users goals when using location-sharing services. By conducting a user study, the researchers were trying to find out when, where, and why users would decide to share their location. Then, these user *goals* were used to suggest new design guidelines because the authors stated that this approach would meet users privacy goals better than current practice of location sharing systems that suggests sharing locations based on *“people’s whereabouts* “[73].

Another interesting paper in the area of locations sharing by Jedrzejczyk et al. [40] suggested “*real-time feedback*” as a new design approach that supports goals when making privacy decisions related to location-sharing. The authors designed a mobile location-sharing/tracking tool that provides users with real-time feedback messages informing them of other users who looked up their location. The tool was tested on families consisting of: parents, young adults children, partners of older children, and family friends. The real-time feedback in this study showed that increased “*awareness* and *visibility”* has affected users’ “*accountability*” when dealing with the system and hence, improved privacy by decreasing the number of “Unjustifiable location requests [40]”. This paper is interesting to the SOUPS community because it shows a better user-centered design solution that has a positive effect on privacy. From an RE point of view, this paper is very interesting because it can serve different RE purposes as follows [40]:

- Stakeholders’ engagement: by studying stakeholders of different age groups and family relationships to accommodate users of different roles who view the system differently. Those stakeholders have different tasks and goals, and they play different roles when dealing with such a system.

- Social effects on requirements: by examining how people interact with systems that have a *social* setting to it, and recruiting participants who engage in a social/family relationships.
- Cognitive effects on requirements: by observing users behavior when information is made visible to them in a way that raises awareness in their cognition.
- Requirements elicitation and analysis: by using data collected from the study to elicit requirements needed for location sharing systems and suggesting design guidelines or *requirements* that are centered on users behavior and their "social criteria [40]". In addition, those suggested guidelines were claimed not to be limited to location-sharing applications, instead they can be generalized and applied to other information sharing applications [40].

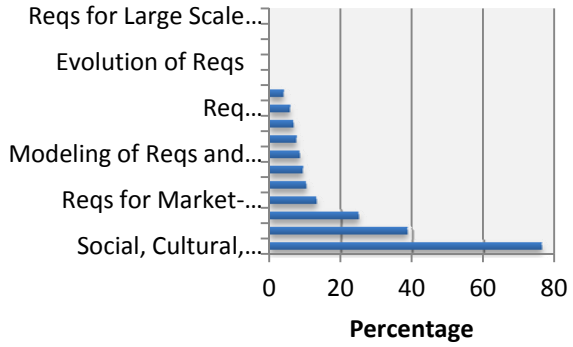


Figure 6. Distribution of topics of interest in SOUPS proceedings

Based on our analysis, we found that 76% of papers published in SOUPS, (see Figure 6) meet the criteria of the "*Social, cultural, global, personal, and cognitive factors in requirements engineering"* category. This result was at no surprise because it can be inferable since the SOUPS call for papers states that it connects the interdisciplinary fields of security and Human-Computer Interaction [89]. The field of HCI takes into consideration all possible factors that can affect users decisions and behaviors when dealing with systems [56]. This classification can be obvious, for example, when SOUPS researchers recruit subjects of family members [40, 15, 57, 34]; study issues of social networking applications [5, 87, 23, 95, 83, 51, 41, 35, 17, 61, 36, 6, 30]; study cognitive sides of passwords requirements and techniques (such as memorability, recall, recognition, etc.) [98, 19, 16, 42, 81, 24, 10, 52, 21, 99, 27, 90, 53, 96]; or conduct studies at different countries around the world to measure the global and cultural impact [72].

"*Requirements elicitation, analysis, verification and validation*" is the next category of requirements topics that ranked high in SOUPS publications: 38% of the total 109 SOUPS papers. We found requirements elicitation and analysis to be present whenever we found a study that collected data from users to use it as an input to document requirements, and/or analyze user input to refine requirements. A good example is a recent paper in the area of smartphone security that conducted a user study on 60 participants in an attempt to derive design recommendations that can be applied to mobile platforms to increase security and usability. Based on the findings and analysis of data from the user study conducted, the authors recommended a list of requirement guidelines for mobile applications such as: user education, backup and remote lock services [11]. The password papers that we mentioned earlier in this Section can be a good example of validation and verification as researchers conduct empirical studies to examine the requirements. [82, 24, 16, 98, 10].

It can be unclear how SOUPS papers would fit into other requirements categories. However, understanding and analyzing the papers' contribution makes the process much easier. For example, the paper: "A "nutrition label" for privacy" [48], proposed a new user-friendly approach that presented privacy policies using visualization derived from the design of nutrition labels found on many consumer products. Let's look at this with the eye of a requirements engineer; the authors are *modeling* privacy requirements by *reusing* a known, well-established framework in another discipline. They took the popular and user-friendly design interface and *repurposed* it to model another area of requirements: privacy policies. In addition to requirements modeling, the paper enhances the end-user training and education because it helps users understand privacy policies better and yet make more informed decisions [48].

## VI. Comparing the Two Research Communities

### A. General goals at abstract level

As we saw from the survey done in both communities, there are goals at the abstract level that can be similar. However, reaching the goals is done differently and that's what distinguishes those two communities from each other. For example, both communities are concerned with privacy requirements and assuring compliance of privacy policies. We can find papers in the RE community describing frameworks that can help with compliance [9, 60], while we find at SOUPS some technical solutions, such as *"privacy nutrition labels"* [48], that help users understand privacy requirements and interpret privacy policy in a user-friendly fashion. Although the two communities here have a similar goal when looking at the bigger picture, means to achieve that goal are different.

### B. Diversity of secuity topics

The diversity of security topics has to do with how security is defined in both communities. In RE, security is defined at a high level. The security sub-topics that RE research touched upon were also defined in a general fashion. On the contrary, the usable security community in SOUPS was trying to expand the classic security definition and to include more areas as the field of security keeps advancing. As already explained in Section V, the "*SOUPS du Jour*" session is a good example of showing SOUPS interest in inviting and adopting new ideas. Mobile security

was a topic under the "*SOUPS du Jour*" session in 2010 [40, 15]. In 2012 proceedings, there was a designated session for mobile privacy and security [11, 33, 25].

### C. Definition of some technical terms

Some terms mean the same thing in both communities such as: privacy requirements, user mental models, stakeholders, etc. However, the research done around issues related to those terms is what's different among RE and usable security. To illustrate, the term "*privacy requirements*" means the same in RE and SOUPS. However, most research in privacy requirements in RE is interested in compliance [9, 60], requirements modeling [59, 46] and analyzing privacy policies of organizations [91]. In SOUPS, privacy requirements research expands more to include stakeholders engagement, for example, where empirical methods are applied to analyze, validate, and verify requirements; and to identify stakeholders, their goals, roles, needs, tasks, etc. [87, 37, 79, 8, 41,]. Another example from SOUPS can be the tool support for Privacy requirements: the community is interested in designing tools that will help model those requirements to stakeholders in a way that helps them understand and make more informed privacy decisions [48, 41].

### D. Evaluation of requirments using emperical studies

As we discussed in Section V, a majority of SOUPS papers conduct empirical studies to test authors' hypotheses, validate current requirements, or to collect data from users for requirements elicitation and analysis. On the other hand, such empirical methods are not widely popular in RE, at least for the 35 security requirements papers that we examined.

### E. Adoption of Invotaive technolgy solutions

As we saw in Section IV.A, the SOUPS community was able to introduce new means to security by adopting new solutions that used *state-of-the-art* technologies such as the use of biometrics for authentication requirements [16]. Security requirements for small devices [54, 43, 32] or smartphones [11, 33, 25] are other examples of leveraging the field to accommodate new technology breakthroughs. We haven't been spotting something similar in the security requirements engineering literature possibly because security-requirements in RE are defining security at the general abstract level.

### F. Relationship to requirements

With regard to requirements classification, Figure 7 shows the percentage of papers published under each of those requirements categories. Percentages here are more accurate than comparing the actual number of papers because the survey sample sizes are not equal among RE and SOUPS. We excluded two categories from the graph: stakeholders and domain-specific problems because we assumed in our analysis that all SOUPS papers meet the requirements criteria for those categories which would make the comparison irrelevant.

According to Figure 7, both communities showed interest in requirements elicitation, analysis, validation and verification (38% Of SOUPS publications and 39% of RE publications), but with different approaching in the research conducted among the two (see Sections IV and V for further explanation).

Figure 7 also shows that there are some requirements topics that the usable security community is not looking into and vice versa. For example, the SOUPS research didn't cover the following: evolution of requirements over time, products families and variability, requirements across the entire system lifecycle, requirements for highly complex systems on a large scale, requirements for large-scale procurement contracts, and the overall RE process. On the other hand, we saw more papers in SOUPS compared to RE addressing areas like "*market-driven approaches*" and "*Social, cultural, global, personal, and cognitive factors in requirements engineering*". In the case of market-driven approaches, the SOUPS community was continuously introducing topics as they become popular in the market. A good example is social networks: from 2011 onwards, we started seeing a special session on social networks because there is an increased popularity in the market for online social networks. We have explained the social, cultural, etc. factors found in SOUPS research in Section V.

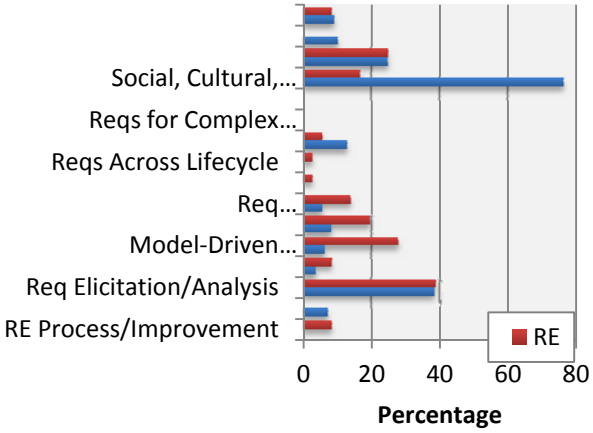


Figure 7. Ratio of RE topics in RE and SOUPS research

### G. Security "by design"

The idea of security by design involves the intentions of creating a secure system from the start by incorporating security from the early stages of development. The SOUPS conference has shown interest this idea. The 2013 call for papers lists "*innovative security or privacy functionality and design*" as the first topic of interest [89]. Our analysis of the SOUPS papers illustrated this interest in the way some authors would support their research by providing design guidelines (see section V for further explanation) [40]. Moreover, research on security topics such as authentication

commonly expressed the need for security to be included in the design of the system. For example, Perković et al. describe the dangers of ignoring security when designing interfaces of authentication schemes [PMJ11].

Because RE involves engaging stakeholders and establishing the groundwork of a system in terms of its requirements in order to set a foundation for design, security research in this area can easily fall into the category of security by design. This can also create a link where RE can support and expand upon such design-related topics in SOUPS.

## VII. Suggestions for Future Research

Based on our findings from the survey, we suggest the following to be considered in future RE research:

### A. Expand security definition

By looking at the SOUPS experience and evolution of security topics over the year, we suggest that the RE community learn from the approach. One might argue that the current general definition of security requirements needs to stay at a higher level because digging into specific areas would possibly be too domain-specific and shift away from the RE view of the world. Although this argument raises a good point, we don't think it is a good idea to keep the security definition as it is now in RE. The security community is currently looking for solutions that will help people and organizations understand and use security [13]. Requirements engineers can help organizations adopt security solutions that meet their stakeholders' goals and needs. Furthermore, an RE process and frameworks for security requirements can act as a form of "*re-usable knowledge*", where solutions can be re-used for different purposes for problems that share a similar context.

### B. Use emperical evidence

Empirical studies have a very good method for testing and validating scientific hypotheses [56]. Requirements validation and verification can benefit a lot from conducting empirical studies. Results of such studies can be used for analysis and elicitation, which in turn can help in creating new requirements or improve the existing requirements. Most importantly, such studies will ensure continuous involvements of stakeholders, which is an essential component of the requirements process [70].

### C. Include innovative technology in research.

Technology is rapidly advancing in every direction. This affects security as well as all types of systems out there. We have seen nice examples in SOUPS where researchers took advantage of new breakthroughs to try to create new ideas that solve current security requirements issues. Researchers in RE can adopt a similar strategy and introduce more innovative solutions in the area of requirements.

### D. Reach out for other communities to find problems that need requirments enginneering research intervention

This can introduce a new research direction for requirements researchers where they can introduce new ideas in new fields. Improving RE process can be a good example where requirements research can benefit usable security: researchers can define an RE process that serves the goals of usable security.

### E. Consider generalizing to other RE areas

Expand the recommendations we provided and the lessons learned from the research we conducted into the security requirement area to create more generalizable solutions that can be applied to other areas of RE.

As with our suggestion of expanding current definition of security, the same idea can be applied to other fields of RE. Researchers can also consider innovative technology breakthroughs similar to what we explained earlier in this section as a way to improve RE research in many fields outside of security requirements.

## VIII. Conclusion

In this paper, we surveyed 35 RE papers that address security requirements. We also surveyed 109 papers published in the SOUPS proceedings to understand how security requirements are being addressed in the usable security community. By compering and contrasting the two, we found some interesting ideas that not only could benefit the security requirements research in RE, but could also inspire other areas of RE research.

## Acknowledgment

This research was funded by the Army Research Office - (W911NF-09-1-0273). We also thank King Abdul-Aziz Univeristy for funding Hanan Hibshi's PhD.

## References

[1] I. Alexander, "Initial industrial experience of misuse cases in trade-off analysis," Proc. IEEE Joint Int'l Conference on Requirements Engineering, 2002, pp. 134-141.

[2] Allen, J. Software Security Engineering: A guide for Project Managers. (2008).

[3] J. S. Anderson and B. Durney, "Using scenarios in deficiency-driven requirements engineering," Proc. IEEE Int'l. Symp. Requirements Engineering, Jan. 1993, pp. 134-141.

[4] A. I. Antón, J. B. Earp, C. Potts, and T. A. Alspaugh, "The role of policy and stakeholder privacy values in requirements engineering," Proc. IEEE Int'l. Symp. Requirements Engineering , 2001, pp. 138-145.

[5] A. Besmer and H. R. Lipford, " Social applications: exploring a more secure framework," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[6] A. Besmer, J. Watson, and H. R. Lipford, "The impact of social navigation on privacy policy configuration ," Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 2010.

[7] Boehm, Barry W. "Software Engineering Economics." IEEE Transactions on Software Engineering. pp.4-21. 1984.

[8] A. Braunstein, L. Granka, and J. Staddon, "Indirect content privacy surveys: measuring privacy without asking about it," Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS), 2011.

[9] T. D. Breaux, M. W. Vail, and A. I. Antón, "Towards regulatory compliance; extracting rights and obligations to align requirements with regulations," 14th IEEE Int'l Conference on Requirements Engineering, Sep. 2006, pp. 49-58.

[10] S. Chiasson, R. Biddle, and P. C. van Oorschot, "A second look at the usability of click-based graphical passwords," Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), 2007, pp. 1-12.

[11] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Balancing Measuring user confidence in smartphone security and privacy," Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS), 2012.

[12] L. Chung, B. A. Nixon, and E. Yu, "Using non-functional requirements to systematically support change," Proc. IEEE Int'l. Symp. Requirements Engineering, Mar. 1995, pp. 132-139.

[13] L. Cranor and S. Garfinkel, Security and Usability: Designing Secure Systems that People Can Use, O'Reilly, 2005.

[14] R. Crook, D. Ince, and B. Nuseibeh, "On modelling access policies: relating roles to their organisational context," Proc. 13th IEEE Int'l Requirements Engineering Conference, Sep. 2005, pp. 157-166.

[15] A. Czeskis, I Dermendjieva, H. Yapit, A. Borning, B. Friedman, and B. Gill, "Parenting from the pocket: value tensions and technical directions for secure and private parent-teen mobile safety," Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 2010.

[16] A. De Luca, M. Denzel, and H. Hussmann, "Look into my eyes!: can you guess my password?," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[17] P. DiGioia and P. Dourish, "Social navigation as a model for usable security," Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS), 2005.

[18] J. S. Downs, M. B. Hollbrook, L. F. Cranor, "Decision strategies and susceptibility to phishing," Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS), 2006.

[19] P. Dunphy, A. P. Heiner, and N. Asokan, " A closer look at recognition-based graphical passwords on mobile devices ", Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 2010.

[20] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic Security Skins," Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS), 2005.

[21] A. E. Dirik, N. Memon, and J. Birget, "Modeling user choice in the PassPoints graphical password scheme," Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), 2007.

[22] G. Elahi and E. Yu, "Trust trade-off analysis for security requirements engineering," 17th IEEE Int'l Requirements Engineering Conference , 2009, pp. 243-248.

[23] S. Fahl, M. Harbach, T. Muders, M. Smith, and U. Sander, "Helping Johnny 2.0 to encrypt his Facebook conversations," Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS), 2012.

[24] A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle, " Improving text passwords through persuasion ", Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS), 2008.

[25] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: user attention, comprehension, and behavior," Proceedings of the 8h Symposium on Usable Privacy and Security (SOUPS), 2012.

[26] V. N. L. Franqueira, T. T. Tun, Y. Yu, R. Wieringa, and B. Nuseibeh, "Risk and argument: a risk-based argumentation method for practical security," 19th IEEE Int'l Requirements Engineering Conference, 2011, pp. 239-248.

[27] S. Gaw and E. W. Felten, "Password management strategies for online accounts," Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS), 2006.

[28] P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone, "Modeling security requirements through ownership, permission and delegation," Proc. 13h IEEE Int'l Conference on Requirements Engineering, Sep. 2005, pp. 167-176.

[29] M. Glinz, "On non-functional requirements," 15th IEEE Int'l Requirements Engineering Conference, Oct. 2007, pp. 21-26.

[30] J. Goecks. W. K. Edwards, and E. D. Mynatt, "Challenges in supporting end-user privacy and security management with social navigation," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[31] C. B. Haley, R. C. Laney, J. D. Moffett, and B. Nuseibeh, "The effect of trust assumptions on the elaboration of security requirements," Proc. 12th IEEE Int'l Requirements Engineering Conference, Sep. 2004, pp. 102-111.

[32] R. Halprin and M. Naor, "Games for extracting randomness," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[33] E. Hayashi, O. Riva, K. Strauss, A. J. B. Brush, and S. Schecter, "Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications," Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS), 2012.

[34] J. T. Ho. D. Dearman, and K. N. Truong, "Improving users' security choices on home wireless networks," Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 2010.

[35] G. Iachello, I. Smith, S. Consolvo, M. Chen, and G. D. Adowd, "Developing privacy guidelines for social location disclosure applications and services," Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS), 2005.

[36] I. Ion, M. Langheinrich, P. Kumaraguru, and S. Čapkun, "Influence of user perception, security needs, and social factors on device pairing method choices," Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 2010.

[37] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun, "Home is safer than the cloud!: privacy concerns for consumer cloud storage," Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS), 2011.

[38] M. Jackson, "The World and the Machine," Proc. 17th Int'l Conf. Software Eng., pp. 283-292, 1995.

[39] R. D. Jeffords and C. L. Heitmeyer, "An algorithm for strengthening state invariants generated from requirements specifications," Proc. IEEE Int'l. Symp. Requirements Engineering , 2001, pp. 182-191.

[40] L Jedrzejczyk. B. A. Price, A. K. Bandara, and B. Nuseibeh, "On the impact of real-time feedback on users' behaviour in mobile location-sharing applications," Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 20109.

[41] S. Jones and E. O'Neill, "Feasibility of structural network clustering for group-based privacy control in social networks,"Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 2010.

[42] M. Just and D. Aspinall, "Personal choice and challenge questions: a security and usability assessment," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[43] R. Kainda, I. Flechais, and A. W. Roscoe, "Usability and security of out-of-band channels in secure device pairing protocols," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[44] R. Kainda, I. Flechais, and A. W. Roscoe, "Two heads are better than one: security and usability of device associations in group scenarios," Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 2010.

[45] E. Kang and D. Jackson, "Dependability arguments with trusted bases," 18th IEEE Int'l Requirements Engineering Conference, 2010, pp. 262-271.

[46] S. Katz and A. Rashid, "From aspectual requirements to proof obligations for aspect-oriented systems," Proc. 12th IEEE Int'l Requirements Engineering Conference, Sep. 2004, pp. 48-57.

[47] D. Karagiannis, J. Mylopoulos, and M. Schwab, "Business process-based regulation compliance: the case of the Sarbanes-Oxley Act,"

15th IEEE Int'l Requirements Engineering Conference, Oct. 2007, pp. 315-321.

[48] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A "nutrition label" for privacy," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[49] Kotonya G. and Sommerville I, Requirements Engineering: Processes and Techniques, United Kingdom; John Wiley & Sons, 1998.

[50] P. Kumaraguru, J. Cranshaw. A. Acquisti. L Cranor, J. Hong, and M. A. Blair, "School of phish: a real-world evaluation of anti-phishing training," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[51] J. King, A. Lampinen, and A. Smolen, "Privacy: is there an app for that?," Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS), 2011.

[52] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[53] C. Kuo, S. Romanosky. L. F. Cranor, "Human selection of mnemonic phrase-based passwords," Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS), 2006.

[54] A. Kobsa, R. Sonawalla. G. Tsudik, E. Uzun, and Y. Wang, "Serial hook-ups: a comparative usability study of secure device pairing methods," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[55] P. Laurent, J. Cleland-Huang, and D. Chuan, "Towards automated requirements triage," 15th IEEE Int'l Requirements Engineering Conference, Oct. 2007, pp. 131-140.

[56] J. Lazar, J. H. Feng and H. Hochheiser: Research Methods in Human-Computer Interaction, Wiley, 2010.

[57] L. Little, E. Sillence, and P. Briggs, "Ubiquitous systems and the family: thoughts about the networked home," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[58] G. Liu, G. Xiang, B. A. Pendleton, J. I. Hong, and W. Liu, "Smartening the crowds: computational techniques for improving human verification to fight phishing scams," Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS), 2011.

[59] L. Liu, E. Yu, and J. Mylopoulos, "Security and privacy requirements analysis within a social setting," Proc. 11th IEEE Int'l Requirements Engineering Conference, Sep. 2003, pp. 151-161.

[60] J. C. Maxwell, A. I. Antón, and P. Swire, "Managing changing compliance requirements by predicting regulatory evolution," 20th IEEE Int'l Requirements Engineering Conference, Sep. 2012, pp. 101-110.

[61] A. Mazzia, K. LeFevre, and E. Adar, "The PViz comprehension tool for social network privacy settings," Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS), 2012.

[62] McConnel, Steve. "From the Editor – An Ounce of Prevention." *IEEE Software 18,3* (May2001):5-7.

[63] J.D. Moffett and B. Nuseibeh, A Framework for Security Requirements Engineering, Technical Report YCS368, Department of Computer Science, University of York, York UK, Aug 2003.

[64] A. Morali and R. Wieringa, "Risk-based confidentiality requirements specification for outsourced IT systems," 18th IEEE Int'l Requirements Engineering Conference, 2010, pp. 199-208.

[65] H. Mouratidis and P. Giorgini, "Secure tropos: A security-oriented extension of the tropos methodology," International Journal of Software Engineering and Knowledge Engineering, World Scientific, 2007.

[66] G. Mussbacher, J. Whittle, and D. Amyot, "Semantic-based interaction detection in aspect-oriented scenarios," 17th IEEE Int'l Requirements Engineering Conference, 2009, pp. 203-212.

[67] J. Mylopoulos. and J. Castro, "Tropos: A Framework for Requirements-Driven Software Development.", Lecture Notes in Computer Science, Springer-Verlag, June 2000.

[68] National Institute of Standards and Technology. "Software Errors Cost U.S. Economy $59.5 Billion Annually" (NIST 2002-10), 2002.

[69] National Institute of Standards and Technology. "Electronic Authentication Guidelines" (NIST 800-63-1), Dec. 2011.

[NGYA06] R. Newman, S. Gavette, L. Yonge, and R. Anderson, "Protecting domestic power-line communications," Proceedings of the 2ndSymposium on Usable Privacy and Security (SOUPS), 2006.

[70] Nuseibeh B., and Easterbrook S., "Requirements Engineering: A Roadmap," The Future of Software Eng., pp. 37-46, 2000.

[71] P. N. Otto and A. I. Antón, "Addressing legal requirements in requirements engineering," 15th IEEE Int'l Requirements Engineering Conference, Oct. 2007, pp. 5-14.

[72] S. Panjwani and E. Cutrell, "Usably secure, low-cost authentication for mobile banking," Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 2010.

[73] S. Patil, G. Norcie, A. Kapadia, and A. J. Lee, "Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice," Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS), 2012.

[74] Ponemon Institute LLC, *2011 Cost of Data Breach Study*, Mar. 2011.

[75] A. Rabkin, "Personal knowledge questions for fallback authentication: security questions in the era of Facebook," Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS), 2008.

[76] RE'13 (2013, Jan 10). *21st IEEE International Requirments Engineering Conference Call for Papers* [Online]. Available: http://www.cin.ufpe.br/~re2013/pages/main.php?id=page_callforpaper

[77] C. Rohleder, "Visualizing the impact of 4on-functional requirements on variants: a case study," 2008 Requirements Engineering Visualization, Sep. 2008, pp. 11-20.

[78] Sasse, M.A. and Flechais, I. "Usable security: Why do we need it? How do we get it?," *O'Reilly*, 2005.

[79] R. Schlegel. A. Kapadia, A. J. Lee, "Eyeing your exposure: quantifying and controlling information sharing for improved privacy," Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS), 2011.

[80] K. Schneider, K. Stapel, and E. Knauss, "Beyond documents: visualizing informal communication," 2008 Requirements Engineering Visualization, Sep. 2008, pp. 31-40.

[81] S. Schechter and R. W. Reeder, "1 + 1 = you: measuring the comprehensibility of metaphors for configuring backup authentication," Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009.

[82] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, and M. L. Mazurek, "Encountering stronger password requirements: user attitudes and behaviors,"Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), 2010.

[83] M. Shehab, S. Marouf, and C. Hudel, "ROAuth: recommendation based open authorization," Proceedings of the 7h Symposium on Usable Privacy and Security (SOUPS), 2011.

[84] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, and J. Hong, "Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish," Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), 2007.

[85] Sindre, Guttorm and Andreas L. Opdahl, Eliciting Security Requirements by Misuse Cases, Proceedings of TOOLS Pacific 2000, 120-131, 20-23 November 2000.

[86] Sindre, Guttorm and Andreas L. Opdahl, Templates for Misuse Case Description, Proceedings of the 7th International Workshop on Requirements Engineering, Foundation for Software Quality (REFSQ'2001), Interlaken, Switzerland, 4-5 June 2001

[87] J. Staddon, D. Huffaker, L Brown, and A. Sedley, "Are privacy concerns a turn-off?: engagement and privacy in social networks," Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS), 2012.

[88] W. Stallings and B. Lawrie, Computer Security: Principles and Practice, 1st ed., Prentice Hall Press, 2007.

[89] Symposium on Usable Privacy and Security (2013, Jan 10). *Ninth Symposium on Usable Privacy and Security Call for Papers* [Online]. Available: http://cups.cs.cmu.edu/soups/2013/cfp.html

[90] F. Tari, A. A. Ozok, S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS), 2006.

[91] R. Tawhid, E. Braun, N. Cartwright, M. Alhaj, G. Mussbacher, and A. Shamsaei, "Towards outcome-based regulatory compliance in aviation security," 20th IEEE Int'l Requirements Engineering Conference, Sep. 2012, pp. 267-272.

[92] A. Toval, A. Olmos, and M. Piattini, "Legal requirements reuse: a critical success factor for requirements quality and personal data protection," Proc. IEEE Joint Int'l Conference on Requirements Engineering, Jan. 1993, pp. 134-141.

[93] T. T. Tun, A. K. Bandara, B. A. Price, Y. Yu, C. Haley, and I. Omoronyia, "Privacy arguments, analysing selective disclosure requirements for mobile applications," 20th IEEE Int'l Requirements Engineering Conference, Sep. 2012, pp. 131-140.

[94] CE. J. Uusitalo, M. Komssi, M. Kauppinen, and A. M. Davis, "Linking requirements and testing in practice," 16th IEEE Int'l Requirements Engineering, Sep. 2008, pp. 265-270.

[ 95] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor, ""I regretted the minute I pressed share": a qualitative study of regrets on Facebook," Proceedings of the 7h Symposium on Usable Privacy and Security (SOUPS), 2011.

[96] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and Nasir Memon, "Authentication using graphical passwords: effects of tolerance and image choice," Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS), 2005.

[97] M. Wu, R. C. Miller, and G. Little, "Web wallet: preventing phishing attacks by revealing user intentions," Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS), 2006.

[98] N. Wright, A. S. Patrick, and R. Biddle, "Do you see your password?: applying recognition to textual passwords," Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS), 2012.

[99] K. Yee, K. Sitaker, "Passpet: convenient password management and phishing protection," Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS), 2006.

[100] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS), 2011.

[101] Zave, P. "Classification of Research efforts in Requirements Engineering," *ACM Computing Surveys*, 29(4): 315-321, 1977.