Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2016, 9, 413-429
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

A Review of Gaps between Usability and Security/Privacy

Majed Alshamari

College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al-Hassa, KSA
Email: smajed@kfu.edu.sa

How to cite this paper: Alshamari, M. (2016) A Review of Gaps between Usability and Security/Privacy. *Int. J. Communications, Network and System Sciences*, **9**, 413-429.
http://dx.doi.org/10.4236/ijcns.2016.910034

Received: May 11, 2016
Accepted: October 22, 2016
Published: October 25, 2016

Abstract

Different domains of computing systems require higher level of focus towards specific quality factors like privacy, integrity, flexibility, usability etc. Moreover, certain quality factors help in each other's existence while others oppose each other significantly. Usability of software applications is one factor that reduces security and privacy up to a substantial level. This paper examines the differences between usability factors and aspects related to security and privacy. A clear understanding of gaps between these two opposing factors has been presented in this paper. In addition, an account of efforts carried out to bridge these gaps has also been presented. We have divided these efforts into the categories of guidelines, frameworks and use of technology. The fields of e-banking and social networks have been considered specifically for identification of gaps in these particular fields.

Keywords

Usability, Software Quality Factors, Security, Privacy, Online Social Networks (OSN)

1. Introduction

A software system usually covers a number of software quality factors and characteristics like privacy, flexibility, user satisfaction, maintainability, usability etc. McCall has divided these factors into three main categories of Product Operation, Product Revision and Product Transition [1]. According to Pressman's definition of Software Quality [2], a quality software system; along with written functional requirements; must also fulfill "implicit characteristics that are expected of all professionally developed software". Moreover, a common observation tells that different software quality factors are strongly associated to each other; for example flexibility helps in better maintenance, and reliability results in increased user satisfaction. However, some characteristics of

software systems conflict with others, an example of which is that usability conflicts with security and privacy. A general assessment discloses that increasing usability usually results in decreased security and privacy [3]-[5]. Similarly, if more attention is given to security and privacy, it usually results in decreased usability.

This paper investigates the conflicts of usability with privacy mainly and with security as well to some level. It also presents a detailed review of proposed methods for reducing the conflicts. The main contribution of this paper is to provide a quick and thorough review for the researchers who want to resolve the conflicts between usability and security/privacy. The paper takes two practical domains as cases for presenting the review; *i.e.* social networking and e-banking. These two domains demand different levels of usability and security/privacy according to their nature of work.

Initially, we set up a definition for our reviewing elements that are usability, security, privacy, e-banking and social networks. Then, the paper presents specific conflicts between usability, security and privacy. Afterwards, an account of research works and efforts focusing on reducing the conflicts has been presented. Later, some research works highlighting the weak areas in social networks and e-banking have also been presented.

Usability has been defined by a number of standards and studies [6] [7], which consider it as a software quality attribute and specify certain characteristics of it. ISO 9241-11 defines usability as, "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" [8]. IEEE standard 1061 is related to Software Quality Metrics and defines usability as, "Usability is the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component" [9]. Jakob Nielsen, a prominent usability expert, defines usability as a quality attribute that depends on five components: Learnability, Efficiency, Memorability, Errors and Satisfaction [10]. Other components of usability can also be found in literature, which include utility, safety, accessibility and some others according to the nature of the software system [11] [12]. Privacy and security also become important usability factors according to the domain of a software system [13]. Examples of such domains are e-commerce, social networking systems, and e-banking.

Privacy in computing or software systems focuses on a number of factors including anonymity of a computer user, sharing of information, access to data etc. [14] [15]. Security works closer to privacy but mainly emphasizes on protection of data from unauthorized usage and safety of users [16] [17]. The factors of privacy and security that this paper mainly considers are user identification, authorization, data privacy and integrity.

Online social networks are websites or systems that provide the facility to their users to build social bonding and relationships in an online sphere. Basic feature of such systems is sharing information and media with other people in the online network [18].

Electronic banking, that is also called online banking or internet banking, is a system that allows its users to conduct different kind of financial transactions and queries by using their computer of mobile devices. It mainly focuses on providing facility to per-

form all possible tasks online that are usually expected to be performed at a bank from client's point of view [19].

2. Usability vs Privacy and Security

As specified earlier, usability is usually inversely related to privacy and security, and these factors have a serious conflict amongst them [20]. The idea that different factors of usability oppose privacy and security has been supported by multiple research works and studies, in different domains including online learning, e-banking, e-commerce and many more [21]-[23]. A basic example of such a conflict is "password", where setting a simple password may be easy to use and to remember, but it creates security concerns. On the other hand, strong passwords are not easy to memorize and recall.

This section presents an account of gaps and conflicts between factors of privacy and security, and usability. Differences between usability and privacy/security can be better examined by dividing these factors into their sub factors. Factors like memorability, learnability, efficiency, errors vs identification, authorization, data privacy, integrity are considered in this paper.

Either we talk about security or privacy, or both of them collectively; there are some major issues that always become obstacle towards increased usability or usable-security. First of all, managing privacy or security online is not the primary goal of users. They always have some other primary task to perform like sharing a photo, transferring money etc. This is why it is difficult to motivate users to learn and perform security and privacy related tasks. Privacy and security settings are treated in an abstract manner and no special attention is given while designing user interface for them. This may lead to mistakenly done privacy or security related actions. Although, for a number of software systems, any unwanted and mistakenly performed action can be undone, however, even after doing something for leakage of private data or breaching of security, one cannot be sure that leakage has not been misused [24]. So, usability problems that become a cause of any mistakenly performed action, may lead to serious privacy or security harms.

System security is an area where user-centered design and user training are least considered [20]. This is one basic reason of the conflict between the two domains. A number of times security professionals are given the task to make an already created system secure. Similarly, many times usability professionals like UI designers or UX experts, also have to enhance usability of already developed systems. This adding-on behavior leads to serious conflicts between usability and security [25]. It is interesting to note that when security of some systems is already an afterthought, enhancing usability of such systems becomes an add-on to an add-on [26]. Pedro and Cristina [27], have specifically formatted the same idea for social networks services development. That the developers of such services usually face pressure related to short development cycles and demand of increased usability, which often results in a compromise on privacy and security of such services.

Because, both usability and security have to be considered earlier in development

process [28]-[30], they should not be treated as final additions to already developed software systems. Considering both usability and security together in the process helps in fixing the conflicts and this concept leads to the idea of usable-security [31], that has been highlighted by multiple research works [32] [33].

Results from a study carried by Prettyman *et al.* show that majority of the people are concerned about security and privacy [34]. However, they do not always act in proper ways to protect their privacy. The goal of the study was to explore how much effort users put to understand and do something to ensure their privacy. Many participants believed that in today's world; that is so interconnected and technologically advanced; there is no question of privacy. That is, whatever they will do, they cannot secure their privacy. Moreover, the results show that most of the users adopt a 'Fatalistic Model' regarding privacy and security, and they believe that their actions will not even harm someone else's privacy. The major reason behind it is that most of the efforts related to privacy focus on the moment when information is released into cyberspace, and not when the user is actually interacting with the information.

Results from a study conducted by Myrthe *et al.* [35] show some significant relationships between usability, visual attractiveness and trust of users on a specific website. Users' trust is also related the perceived usability of a website, that in most cases is strongly related to actual usability. Aries *et al.* [36] also support the relationship between trust and usability of e-banking websites specifically. According to their study, website usability has a strong relationship with trust, however relationship of initial perceived usability and trust is not much significant. The reason behind this is that the factor of trust is developed over the period of time.

Although, it is widely known that different applications have different requirements of usability and privacy, however, even specific users in the same online community or social network may have different opinions and requirements of privacy [37]. For example, a specific user may not be bothered if other users add him to their social circle, whereas some users may not want it and consider it as a privacy issue. Although, this issue is addressed by many online social networks including Facebook, still it has to be understood by service providers. Furthermore, some users may be even concerned about their online privacy, but still they have to share their information to reach their goals (like, sharing information on LinkedIn). Moreover, even the users are concerned about their privacy and security; still they are attracted towards better usable applications/systems. An example of this is the interest of users in Android and Apple systems, even though BlackBerry or Microsoft's Windows Mobile are more secure.

3. Bridging the Gaps between Usability and Privacy/Security

In the previous section, we highlighted the gaps and conflicts between security/privacy and usability. Different efforts have been made to reduce the conflicts and bridge the gaps. In this section, we summarize such efforts made in specific domains or in general. We categorize these efforts in three groups:

- Guidelines/recommendations for reducing the gaps

- Frameworks/Models
- Use of technology to remove the conflict

3.1. Guidelines for Reducing the Gaps

Different research studies have come up with set of guidelines and procedures to be followed in order to reduce the gaps between usability and privacy/security. F. Sahar [38] has presented a set of guidelines that considers the tradeoffs between usability attributes and security. Different factors of usability like effectiveness, efficiency, satisfaction and learnability have been evaluated against security and guidelines focusing on general concepts of right tradeoffs have been provided. For a better tradeoff between effectiveness and security, concepts related to security should be considered in early stages. For better satisfaction and security, trust should be provided on ease of use as well as on security aspects especially transactions and payments. Satisfaction is one attribute of usability that is directly proportional to security in many cases. For example, a user will be more satisfied if he knows that a banking transition is secure and safe. In case of efficiency and security, one must consider speed and accuracy in security tasks. Sometimes it gets difficult as additional tasks related to security (e.g. authentication) have to be performed that increase overall task time. For a correct tradeoff between learnability and security, learnability should be given more importance. Difficult to learn security aspects lead to lack of user motivation to complete tasks. Moreover, for better security, users must learn the tasks properly in order to avoid mistakes that lead to security issues. Examples of this can be, accidental information breach, wrong transactions etc. [25].

Another set of guidelines for usability of security mechanisms has been presented by Hans-Joachim [26] that focuses on providing a checklist for software developers of security systems. Understandability is considered as the first and very important factor as the end user must be able to understand the security mechanism. Although, end users do not often know such mechanisms technically, but they must be able to at least comprehend what ever mechanism is visible to them. A good practice is to hide as many as possible security related tasks from the users. Secondly, users must feel that they are controlling the system. Offering multiple ways for handling the security of the system is one way to accomplish this, however, security should not be compromised in any of the ways. Another presented guideline is to reduce the memory load of the user, related to security mechanisms. Users do not like to remember too much information, that's why required memorization should be reduced as much as possible. Maximum number of security related decisions should be made by the system; a user should only be asked for a decision when it is clear to the user and they are capable of deciding specifically about it. Further guidelines include proper reaction on user errors, consistent behavior of security mechanisms, default security settings and reduced fear of security failure.

Not only security and usability should be considered together as usable security, but also they should be evaluated together in order to get a clear picture about the effectiveness of systems focusing on security. Martin *et al.* [39] have presented some guide-

lines to evaluate usable security in a quantifiable manner focusing on factors of security and usability. The idea is to evaluate security and usability alongside in order to assess aspects of both factors. For both quality dimensions; *i.e.* security and usability; parameters are determined that are used as quality criteria. For each quality criteria a deficiency value of 0 to 1 is measured (0 being high deficiency and 1 as no deficiency). Quality criteria for security include secrecy, privacy, revelation and breakability. And quality criteria for usability include meaningful retrieval, depth of processing, and convenience. It can be observed that for evaluating usable security, usability factors have to be carefully selected that are closer to security. General usability factors cannot be as effective for a proper evaluation.

3.2. Frameworks/Models

Apart from guidelines, different frameworks and models can also be found in literature, that assist in addressing the conflicts between usability and security/privacy. An ontological approach has been presented by Mairza *et al.* [40] that focuses on managing the conflicts between security and usability requirements. The ontology helps in determining the impacts of conflict between security and usability, and also in selecting relevant strategies to resolve the conflict. The flow of the proposed ontological framework, as shown in **Figure 1**, starts with the identification of security and usability requirements, system context and domain of application. After that identifying the existence of conflicts is taken in to consideration. Once identified, the conflicts are categorized according to their impacts, and lastly conflict resolution strategies are formulated according to application domain.

Different websites and systems have their agreed and formulated privacy policies, however, it is a very common observation that general users never tend to specifically focus on these policies. As a result, most of the users stay unaware of what the website/system may share about them or from their data. Furthermore, most of the times when some information is shared, the owner of the information is usually not informed, because it has already been specified in the privacy policy. Han-Gyu Ko *et al.* have presented [41] a usability enhanced privacy protection system that is based on users' responses. The proposed system tries to use the concept of Federated ID Management (FID) that has been discussed later in this paper. According to the proposed system, whenever personal information of any user has to be released, the system sends a consent message to the user specifying the purpose of release of information. Based on the response of user, the decision for releasing the information is made. Although, the user can control information release very properly through the proposed idea, however, it becomes a time consuming process. Availability of the user to respond to information release query is also a question.

Shih-Wei *et al.* [42] have presented a model for simplifying the privacy settings of Facebook and making them more user-friendly. The idea is to let all users manage their privacy settings, without even having much knowledge of these settings. The model divides privacy settings in hierarchical manner and defines three levels of privacy as basic,

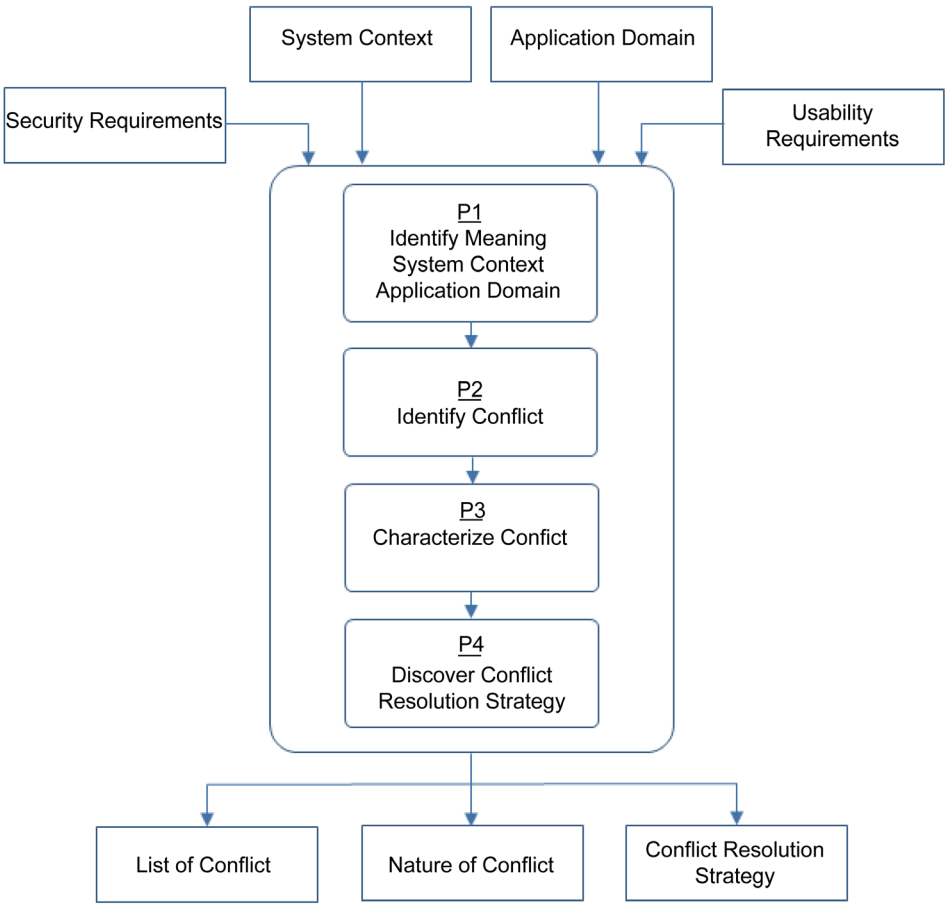

Figure 1. Framework for security-usability requirements conflict management.

medium and advanced. The basic level focuses on securing the users' privacy from unknown users, and all users should at least select this basic level of privacy settings. Medium level ensures to secure information from friends of friends, advertisers and other third parties. Advanced level is the most secure and private level that even prevents privacy attacks from friends and it also minimizes information disclosure. This simple approach of pre-defined privacy levels increases the usability of privacy settings as well as tries to keep away the user from details of these settings by offering him a simple mechanism of hierarchical privacy settings. Similar kind of models can be used by social networks other than Facebook.

One of the very important factors in privacy is confidentiality. A huge number of users nowadays use cloud services in order to store and share information. A number of social network services encourage people to share their personal information in multiple forms. According to Sascha *et al.* [43] users of online cloud services including social networks fail to consider privacy issues properly. Although, there are multiple approaches to address privacy and confidentiality issues in cloud, still they are not properly adopted due to lack of awareness as well as usability issues. Sascha *et al.* have presented a new idea of "Confidentiality as a Service" (CaaS) for cloud platforms. Accord-

ing to this model, confidentiality is taken care of by another service provider on cloud. CaaS must also focus on usability and should not conflict with already known usage patterns. The basic idea of the proposed approach is to send the required data to a Caas provider before sharing it with other users through a social network. CaaS provider adds a confidentiality layer to the information/data that is shared. The receivers of the data will also require CaaS provider in order to remove the confidentiality layer and view actual data as shown in **Figure 2**. The presented model focuses on multiple usability aspects as usability is considered as a closely related factor to confidentiality in specific and privacy in general. For this reason, the model focuses on integrating the approach into the users' usage patterns. Even if the credentials for decryption are lost, the user must be able to recover the data. And the users must be able to access encrypted data from multiple devices. This model is an example of increased focus on privacy concerns while addressing usability aspects as well.

A security-usability threat model has been presented in [44] that focuses on HCI Security (HCISec). HCISec is centered around the user, who demands security as well as usability. Therefore, HCISec model must be different from traditional security threat models, and it must incorporate usability factors in addition to general security factors. The study presents a basic security-usability threat model that provides critical factors to be investigated for evaluation of security and usability. The model provides important factors for security and usability, and some common factors that are related to security as well as usability. Security-usability threat model has been represented in **Figure 3**. Moreover, the presented model also provides a methodology for identifying usability and security threats, based on usage scenarios and threat scenarios. Usage scenarios help in identifying areas that decrease usability of the system, whereas threat scenarios help in identification of security threats to the system.

Assessment framework for usable-security (AFUS) [45], is another effort for balancing usability and security based on techniques from Decision Science domain. AFUS workflow starts with filtering and merging requirements related to usability and security, followed by using utility functions for decision and risk analysis related to utility of

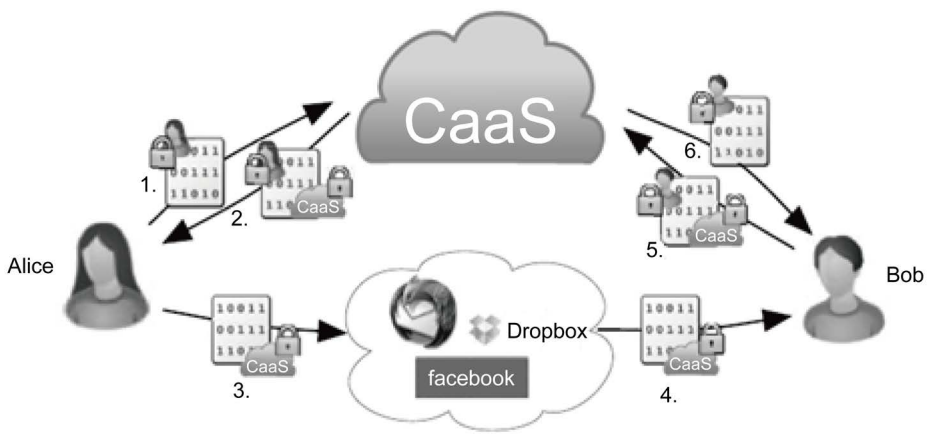

Figure 2. Basic idea of Confidentiality as a Service (CaaS).

attributes of security, usability and usable-security. Afterwards, decision trees are used to calculate the weights and utility value of each attribute. These values help in filtering and selecting the most important attributes to be used in requirements specification of a software product. Requirements specified after using AFUS have an acceptable balance between factors of usability, security and usable-security. Pictorial representation of AFUS has been presented in Figure 4.

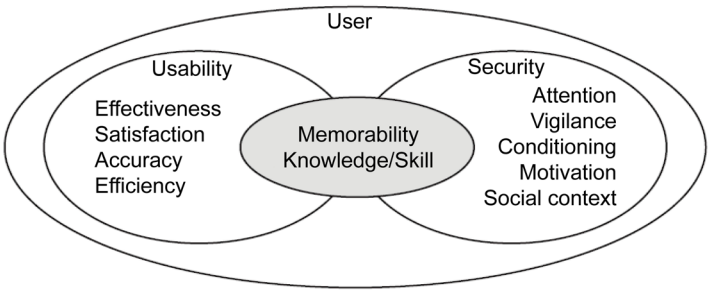

Figure 3. Basic idea of Confidentiality as a Service (CaaS).

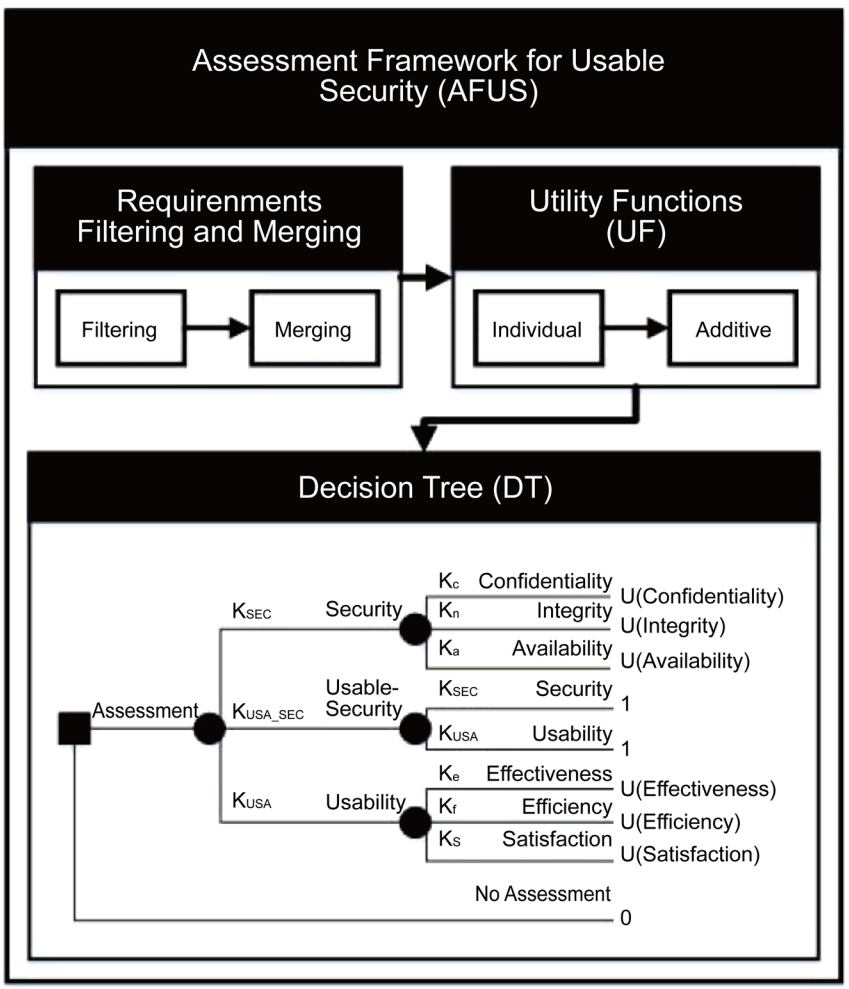

Figure 4. Assessment Framework for Usable-Security (AFUS).

3.3. Use of Technology

This section gives an account of efforts made for solving the issue of gaps between usability and privacy/security using technology. These include all practical efforts including implementing new ideas, designing new paradigms or proposing technical methods for the said issue.

Most of the internet users nowadays have accounts on different online services including social networks, mailing service providers and others. Having same password for all accounts is a serious security concern, and on the other hand remembering different passwords is very difficult and is referred to as "password fatigue". Federated ID Management (FID), tries to address this issue, by enabling users to use same ID across different applications. A user of one network/application can access information of another through this idea. Three main concepts/entities in this regard are:

Service Provider (SP): That provides any service like social networking, messaging, calling etc. It is also called Relying Party (RP).

Identity Provider (IDP): Another website or service which provides or verifies the identity of the user.

User Agent (UA): A web browser or other software that communicates with a remote system on behalf of the user.

Different efforts to implement the concept of FID have been made including BrowserID, Open ID and WebID. BrowserID uses an email address as a user's unique ID. Email addresses are common and users are used to it. Using unique URIs looks foreign and users feel reluctant using them. WebID aims to develop a platform for creating a distributed social network. A user must prove ownership of a URI for verifying his ID. Client certificate verification mechanism is used. All modern browsers have this feature commonly known as Secure Socket Layers (SSL). Hackett *et al.* [46] have analyzed some concerns related to BrowserID and WebID. Device loss is an important concern where user's information and accounts get on stake if the device is lost. They have also specified usability as a major issue because perceived complexity by average users is very high. The concept of FID cannot be successful until general users accept it because user experience is mainly responsible for a technology's success.

Multiple accounts and use of multiple online services is not only an issue for the users, but on the other hand it is also a concern for service providers that their services are being used by genuine users. Xiang Zou and Bo Jin [37] formulate that real identity of users can be different from the identity they provide online and at times users may not want to disclose their real identity on the internet as well. Real world identity of a user is termed as trusted electronic identity (TrEid), whereas there can be multiple false identities that are termed as common electronic identity (CoEid). The research work highlights the idea of mutual trust between service providers (SP) and users. SPs must be assured that trustworthy users are using their services, and on the other hand, users must have the trust that privacy, confidentiality and integrity is preserved by the SPs. An approach based on identity management with trust relationship is proposed where the user can generate one TrEid to gain the trust of an SP, and then he may be allowed

to use multiple CoEids to preserve his identity online. TrEid may be kept confidential and may not be shared with other online users. This provides a balance of trust between SPs and users; where SPs can ensure genuine users, and users may keep using services without disclosing their real world identity.

Social network users keep posting bulk of information and data on daily basis. This data is used by service providers as well to provide user better facilities. Different trades and businesses also demand access to specific information about users in order to advertise their products. Moreover, this data can also be positively utilized for social analysis. However, users' privacy gets on risk through this process and it must be ensured that no information is misused. In order to give benefits to both parties (users and other business) a balanced approach must be adopted. First of all it must be clear to the user that how data is used and who is having access to it. Secondly, data degradation can be used that focuses on storing data in less accurate forms that is least sensitive to privacy leakage issues [47]. Data generalization also refers to the approach where data is stored in forms of summaries and actual data is not represented. With this method, OSN providers can even provide data to different trades and businesses without threatening privacy of users.

The studies and research works presented in this section span over multiple areas related to the conflicts between usability and privacy/security. We believe that adopting a single way to bridge the gaps between highlighted domains is not enough and efforts from multiple dimensions should be made. A possible explanation to this can be the consideration of usability and security requirements in the initial phase of software development, as well as following the guidelines during the development life cycle, and also focusing on presenting new ways to reduce the distances between the said areas. Different domains have their own usage patterns as well as security requirements and levels of privacy. So, a single set of guidelines or a sole framework is not enough to address issues of every particular domain.

4. Weak Areas in Social Networks and E-Banking

In this section, we summarize the presented discussion in terms of social networks and e-banking. Potential issues related to usability and privacy/security in these two domains have been highlighted. Moreover, research works specifically related to the mentioned domains have also been included in this section.

Madejski *et al.* conducted a research about online social networks' (OSN) privacy settings and their practice by [48] the website's users. It has been discussed that different social networks provide privacy settings through which users may control what they want to share and with whom. However, users of such websites usually fail to do so due to flaws and loopholes in privacy settings of social media websites. The research analyzes privacy settings of different users against their sharing intentions. Majority of the participants (users) thought that their privacy settings are correct, though, it was not actually. 93.8% participants revealed some information that they did not want to disclose. 84.6% participants mistakenly concealed some information that they actually

wanted to share. The research concludes that user interface design is working against the purpose of privacy settings of online social networks. An important factor to consider is that different social networks (including Facebook), offer privacy settings based on type of data (photos, videos, status etc.), however, in actual life it is based on context (sorrow, happiness, success etc.). Although, users can manage privacy of each data item separately, yet a better approach for privacy settings can be one that focuses on context of information to be shared rather than data type.

Similar results have also been presented by Yabing and Krishna [49] showing that only 37% of the times, privacy settings match users' expectations. And almost always when it does not match, it leads to revealing information to someone it was not supposed to. Moreover, the results also show that even the users who are concerned about their privacy and who also change their privacy settings, still fail to set their privacy settings properly. Even the changed privacy settings match user expectations 39% of the times only. This also indicates that although OSNs are indeed popular and attract a number of users, still they have to focus on usability of privacy settings, so that their users become able to achieve what they actually want.

The research by Paul *et al.* [50] also highlights the same issue that users of social networking websites (specifically Facebook) face trouble in understanding and configuring privacy settings. Many research works have shown that most of the users of social networks keep using default privacy settings and never change them [51]-[53]. A major reason for this is low usability of privacy settings that even causes over-sharing of information. The research presents a new privacy based interface that focuses on three criteria; users should be able to change privacy settings with very little effort; common practices like should be applied for designing privacy settings; and color coded interface should be used for better usability of privacy settings user interfaces. The suggestions of the research can be considered by social networks in order to enhance usability of their privacy settings. Multiple improvements have already been made by Facebook particularly, like excluding specific users from viewing certain posts, and adjusting visibility of specific items separately. Another, strong suggestion can be offering groups based privacy settings, where a user may or may not share specific information with certain group of users/friends.

Along with different other research works, the study of Zhang Chi *et al.* [54] also states that there are design conflicts between security/privacy and basic goals of social networks *i.e.* usability and sociability. Most of the users create profiles on social media in order to share information and to interact socially. For being active and noticed on social networks, it is almost necessary for users to keep sharing information. But, while doing so a number of users accidentally reveal information to such users, to which they actually did not intend to [48]. A balance between security/privacy and usability factors is necessary and it is mainly dependent on particular purpose of using an online social network. A social media website or app has to offer and facilitate multiple elements for proper social interactions. These include personal space management, social content management, communication means and different kinds of searching options. These

factors mainly focus on usability and sociability, but for privacy and security further features related to users' identity anonymity, personal space privacy, communication privacy and data integrity should also be included in an OSN.

Although, it is a general perception that privacy and security would matter a lot in e-banking, however, results from the some studies [55], [56] show that privacy and security are least concerned by the users at times. According to [55], security is not having any significant relationship with intention to use online banking services. The reason is that most of the users perceive that an online banking website is secure by default. Similarly, according to [56], users' responses do not show that they care about privacy in e-banking, which is a misleading result according to the study itself. The main reason behind this is that privacy policies are poorly written and fail to engage users. The analysis of the results suggests that new ways to specify privacy policies must be designed that are easy to use and better understandable by general users.

In light of the studies and works reviewed above, usable security and privacy in the fields of social networks and e-banking should be considered reasonably. These domains, especially social networks is an example of such fields where privacy and security matter a lot, yet the system has to be usable enough to offer acceptably good services to its users.

5. Conclusion and Future Work

In this paper, we presented a review of how usability is related to security/privacy. Most of the studies consider usability as a factor that conflicts privacy and security. The existence of one factor usually discourages the other. The fact has been addressed by a number of studies, and efforts have been made to reduce the gaps between the mentioned conflicting factors.

We have divided these efforts in three categories; first as some basic guidelines for reducing the gap, second as presented frameworks and models, and third as use of technology to bridge the identified gaps in different domains.

The paper also highlights that specific domains as social media and e-banking are very much affected by the gaps between usability and privacy/security. Because in such domains the role of privacy or security is very important, yet they are supposed to be highly usable to facilitate their users.

It is expected that in future security measures and features to be included in software systems would directly address usability concepts, as the demand for usable and efficient systems has highly increased. New usage patterns could also be introduced that do not conflict with security and privacy principles.

In future, we plan to specifically focus this research towards e-Banking in Saudi Arabia. Saudi Arabian Monetary Agency (SAMA) has provided a detailed set of e-Banking guidelines for banks operating in Saudi Arabia. We intend to investigate the relationships between these guidelines and usability vs. security/privacy issues as highlighted in this paper. Moreover, we also expect to propose a usability oriented set of recommendations to be followed by Saudi Arabian banks.

References

[1] McCall, J.A., Richards, P.K. and Walters, G.F. (1977) Factors in software quality. Volume I. Concepts and Definitions of Software Quality. General Electric Co., Sunnyvale, CA.

[2] Pressman, R.S. (2005) Software Engineering: A Practitioner's Approach. Palgrave Macmillan, London.

[3] Fléchais, I. (2005) Designing Secure and Usable Systems. Dissertation, University College London.

[4] Madejski, M., Johnson, M.L. and Bellovin, S.M. (2011) The Failure of Online Social Network Privacy Settings. https://mice.cs.columbia.edu/getTechreport.php?techreportID=1459

[5] Zhang, C., *et al.* (2010) Privacy and Security for Online Social Networks: Challenges and Opportunities. *IEEE Network*, **24**, 13-18. http://dx.doi.org/10.1109/MNET.2010.5510913

[6] Abran, A., *et al.* (2003) Usability Meanings and Interpretations in ISO Standards. *Software Quality Journal*, **11**, 325-338. http://dx.doi.org/10.1023/A:1025869312943

[7] Quesenbery, W. (2001) What Does Usability Mean: Looking beyond Ease of Use. *Proceeding of* 48*th Annual Conference-Society for Technical Communication*, Chicago, 13-16 May 2001.

[8] ISO 9241-11:1998 (1998) Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs). The International Organization for Standardization, Geneva.

[9] Geraci, A., *et al.* (1991) IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.

[10] Nielsen, J. (2003) Usability 101: Introduction to Usability. https://www.nngroup.com/articles/top-10-mistakes-web-design/

[11] Febretti, A. and Garzotto, F. (2009) Usability, Playability, and Long-Term Engagement in Computer Games. *CHI*'09 *Extended Abstracts on Human Factors in Computing Systems*, 4063-4068. http://dx.doi.org/10.1145/1520340.1520618

[12] Iwarsson, S. and Ståhl, A. (2003) Accessibility, Usability and Universal Design—Positioning and Definition of Concepts Describing Person-Environment Relationships. *Disability and Rehabilitation*, **25**, 57-66.

[13] Tilson, R., *et al.* (1998) Factors and Principles Affecting the Usability of Four E-Commerce Sites. *Proceedings of the* 4*th Conference on Human Factors & the Web*, Basking Ridge, New Jersey.

[14] http://www.computerhope.com/jargon/p/privacy.htm

[15] https://www.techopedia.com/definition/24954/internet-privacy

[16] http://www.webopedia.com/TERM/S/security.html

[17] http://its.ucsc.edu/security/training/intro.html

[18] http://www.journals.elsevier.com/social-networks/

[19] http://www.investopedia.com/terms/o/onlinebanking.asp

[20] Just, M. (2010) Security and Usability. School of Informatics, University of Edinburgh, Edinburgh.

[21] Ivanovic, M., *et al.* (2013) Usability and Privacy Aspects of Moodle: Students' and Teachers' perspective. *Informatica*, **37**, 221-230.

[22] Montazemi, A.R. and Hamed, Q. (2015) Factors Affecting Adoption of Online Banking: A Meta-Analytic Structural Equation Modeling Study. *Information & Management*, **52**, 210-226. http://dx.doi.org/10.1016/j.im.2014.11.002

[23] Majid, R.A.L., Mardziah, H. and Nurul A'syida Abdul, J. (2014) An Evaluation on the Usability of E-Commerce Website Using Think Aloud Method. *New Perspectives in Information Systems and Technologies*, **2**, 289-296. http://dx.doi.org/10.1007/978-3-319-05948-8_28

[24] Whitten, A. and Tygar, J. (1999) Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. *Proceedings of the* 8*th USENIX Security Symposium*, **8**, 14.

[25] Yee, K.-P. (2004) Aligning Security and Usability. *IEEE Security & Privacy*, **5**, 48-55.

[26] Hof, H.-J. (2015) User-Centric IT Security—How To Design Usable Security Mechanisms. arXiv preprint arXiv:1506.07167

[27] Pimenta, P.C. and De Freitas, C.M. (2010) Security and Privacy Analysis in Social Network Services. 5*th Iberian Conference on Information Systems and Technologies* (*CISTI*), Santiago de Compostela, 16-19 June 2010, 1-6.

[28] Parveen, N., Rizwan, B. and Khan, M. (2014) Integrating Security and Usability at Requirement Specification Process. *International Journal of Computer Trends and Technology*, **10**, 236-240. http://dx.doi.org/10.14445/22312803/IJCTT-V10P142

[29] Holzinger, A. (2005) Usability Engineering Methods for Software Developers. *Communications of the ACM*, **48**, 71-74. http://dx.doi.org/10.1145/1039539.1039541

[30] Devanbu, P.T. and Stuart, S. (2000) Software Engineering for Security: A Roadmap. *Proceedings of the Conference on the Future of Software Engineering*, Davis, 4-11 June 2000, 227-239. http://dx.doi.org/10.1145/336512.336559

[31] Balfanz, D., *et al.* (2004) In Search of usable Security: Five Lessons from the Field. *IEEE Security & Privacy*, **5**, 19-24. http://dx.doi.org/10.1109/MSP.2004.71

[32] Garfinkel, S. and Heather, R.L. (2014) Usable Security: History, Themes, and Challenges. Synthesis Lectures on Information Security, Privacy, and Trust. Morgan & Claypool Publishers, San Rafael, 1-124. http://dx.doi.org/10.2200/S00594ED1V01Y201408SPT011

[33] Cranor, L.F. and Norbou, B. (2014) Better Together: Usability and Security Go Hand in Hand. *IEEE Security & Privacy*, **6**, 89-93. http://dx.doi.org/10.1109/MSP.2014.109

[34] Prettyman, S.S., *et al.* (2015) Privacy and Security in the Brave New World: The Use of Multiple Mental Models. In: Tryfonas, T. and Askoxylakis, I., Eds., *Human Aspects of Information Security, Privacy, and Trust*, Springer, Berlin, 260-270. http://dx.doi.org/10.1007/978-3-319-20376-8_24

[35] Swaak, M., De Jong, M. and De Vries, P. (2009) Effects of Information Usefulness, Visual Attractiveness, and Usability on Web Visitors' Trust and Behavioral Intentions. *IEEE International Professional Communication Conference*, Waikiki, 19-22 July 2009, 1-5. http://dx.doi.org/10.1109/ipcc.2009.5208719

[36] Susanto, A., Lee, H. and Zo, H. (2011) Factors Influencing Initial Trust Formation in Adopting Internet Banking in Indonesia. 2011 *International Conference on Advanced Computer Science and Information System* (*ICACSIS*), Jakarta, 17-18 December 2011, 305-310.

[37] Zou, X. and Jin, B. (2010) Identity Management with Trust Relationship and Privacy Preservation. 2010 *IEEE International Conference on Information Theory and Information Security* (*ICITIS*), Beijing, 17-19 December 2010, 366-370.

[38] Farrukh, S. (2013) Tradeoffs between Usability and Security. *IACSIT International Journal of Engineering and Technology*, **5**, 536-540.

[39] Mihajlov, M., Blažič, B.J. and Josimovski, S. (2011) Quantifying Usability and Security in Authentication. 2011 IEEE 35*th Annual Computer Software and Applications Conference*

(*COMPSAC*), Munich, 18-22 July 2011, 626-629. http://dx.doi.org/10.1109/COMPSAC.2011.87

[40] Mairiza, D. and Zowghi, D. (2010) An Ontological Framework to Manage the Relative Conflicts between Security and Usability Requirements. 2010 3*rd International Workshop on Managing Requirements Knowledge* (*MARK*), Sydney, 27 September 2010, 1-6. http://dx.doi.org/10.1109/MARK.2010.5623814

[41] Ko, H.-G., Kim, S.-H. and Jin, S.-H. (2007) Usability Enhanced Privacy Protection System Based on Users' Responses. *IEEE International Symposium on Consumer Electronics*, Las Vegas, 10-14 January 2007, 1-6. http://dx.doi.org/10.1109/isce.2007.4382188

[42] Fang, S.-W., Rajamanthri, D. and Husain, M. (2015) Facebook Privacy Management Simplified. 2015 12*th International Conference on Information Technology-New Generations* (*ITNG*), Las Vegas, 13-15 April 2015, 719-720. http://dx.doi.org/10.1109/ITNG.2015.121

[43] Fahl, S., *et al.* (2012) Confidentiality as a Service—Usable Security for the Cloud. 2012 IEEE 11*th International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom*), Liverpool, 25-27 June 2012, 153-162. http://dx.doi.org/10.1109/TrustCom.2012.112

[44] Kainda, R., Flechais, I. and Roscoe, A.W. (2010) Security and Usability: Analysis and Evaluation. *International Conference on Availability, Reliability, and Security*, Krakow, 15-18 February 2010, 275-282. http://dx.doi.org/10.1109/ARES.2010.77

[45] Hausawi, Y.M. and Allen, W.H. (2014) An Assessment Framework for Usable-Security Based on Decision Science. *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Heraklion, 22-27 June 2014, 33-44. http://dx.doi.org/10.1007/978-3-319-07620-1_4

[46] Hackett, M. and Kirstie, H. (2012) Security, Privacy and Usability Requirements for Federated Identity. *Web* 2.0 *Security & Privacy Workshop*, **2**.

[47] Van Heerde, H., Maarten, F. and Nicolas, A. (2009) A Framework to Balance Privacy and Data Usability Using Data Degradation. *International Conference on Computational Science and Engineering*, **3**, 146-153. http://dx.doi.org/10.1109/cse.2009.174

[48] Madejski, Mi., Maritza Lupe, J. and Bellovin, S.M. (2011) The Failure of Online Social Network Privacy Settings.

[49] Liu, Y., et al. (2011) Analyzing Facebook Privacy Settings: User Expectations vs. Reality. *Proceedings of the* 2011 *ACM SIGCOMM Conference on Internet Measurement Conference*, Berlin, 2-4 November 2011, 61-70. http://dx.doi.org/10.1145/2068816.2068823

[50] Paul, T., Puscher, D. and Strufe, T. (2011) Improving the Usability of Privacy Settings in Facebook. arXiv:1109.6046

[51] Bilge, L., *et al.* (2009) All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. *Proceedings of the* 18*th International Conference on World Wide Web*, Madrid, 20-24 April 2009, 551-560. http://dx.doi.org/10.1145/1526709.1526784

[52] Catanese, S.A., *et al.* (2011) Crawling Facebook for Social Network Analysis Purposes. *Proceedings of the International Conference on Web Intelligence, Mining and Semantics*, Sogndal, 25-27 May 2011, Article No. 52. http://dx.doi.org/10.1145/1988688.1988749

[53] Strufe, T. (2010) Profile Popularity in a Business-Oriented Online Social Network. *Proceedings of the* 3*rd Workshop on Social Network Systems*, Paris, 13-16 April 2010, Article No. 2. http://dx.doi.org/10.1145/1852658.1852660

[54] Zhang, C., *et al.* (2010) Privacy and Security for Online Social Networks: Challenges and Opportunities. *IEEE Network*, **24**, 13-18. http://dx.doi.org/10.1109/MNET.2010.5510913

[55] Cooharojananone, N., Chofa, S. and Phimoltares, S. (2011) A Study on Intention to Use Factor in the Internet Banking Websites in Thailand. 11*th International Symposium on Applications and the Internet* (*SAINT*), Munich, 18-21 July 2011, 556-561. http://dx.doi.org/10.1109/saint.2011.103

[56] Costante, E., Den Hartog, J. and Petkovic, M. (2011) On-Line Trust Perception: What Really Matters. 1*st Workshop on Socio-Technical Aspects in Security and Trust* (*STAST*), Milan, 8 September 2011, 52-59. http://dx.doi.org/10.1109/STAST.2011.6059256