A Framework for Evaluating Usable Security: The Case of Online Health Social Networks

A. Yeratziotis, D. van Greunen and D. Pottas

Institute for ICT Advancement, Nelson Mandela Metropolitan University, Port Elizabeth, Eastern Cape, South Africa
e-mail : alexandros.yeratziotis@nmmu.ac.za

Abstract

It is vital that the development of security and privacy features for applications and websites are assessed for their usability. An assessment of such usability will increase the continuous and effective utilisation from the user perspective. However, owing to a lack of tools and methods this is difficult to achieve. There is thus a need for a usable security framework to facilitate the usability assessment of security and privacy features for applications and websites. This paper discusses such a framework within the context of online social networks that are particular to the health domain. The framework consists of three components: a three-phase process, a validation tool and a usable security heuristic evaluation. The paper begins by providing an overview of the complete conceptualised framework, which is followed by a more detailed discussion of the components.

Keywords

Framework, usable security, heuristic evaluation, validation tool, three-phase process, online health social networks.

1 Introduction

Reality is that current security and privacy features make unreasonable demands on users, system administrators and developers alike (Sasse and Flechais, 2005). Accordingly, keeping a system's or users' personal information secure involves an increasing amount of complexity. Owing to the complexity, users avoid interacting with the available security and privacy features on websites and applications; consequently providing attackers with an even greater advantage. Developers struggle because they are not aware of the security implications of their design decisions; yet, they are the ones left with the responsibility for making security decisions and designs for these new applications and websites.

The field that investigates the complexities that users experience when interacting with security is usable security. It embraces the fact that most applications and websites have security features that users should interact with. However, due to their lack of usability, users often avoid and even ignore their security responsibilities (Furnell, Jusoh and Katsabas, 2006). The non-usable design of security has contributed to the fact that the human is regarded as the most common cause behind security configuration errors, which undermine the overall security (Furnell et al., 2006; Whitten and Tygar, 2005). It is evident that there is a problem in the interaction between the human element and the technology (design of the interface). This problem relates to the research discipline of human-computer interaction as much as it does to the discipline of information security. In essence, developing security that is usable has become a necessity and is well supported (Furnell et al., 2006; Whitten and Tygar, 2005).

Properties that define usable security have been determined based on the cumulative knowledge available in this research space. For an application/website to be usable from a security and privacy perspective, users must be consistently and reliably made aware of the security-related tasks they need to perform, users must be able to easily determine how to accomplish the necessary tasks successfully, users must not be prone to making any dangerous errors and users must be comfortable with the user-interface if they are to continue to use it (Yee, 2002; Whitten and Tygar, 2005).

2 Problem and Research Questions

Theories and evaluation tools for usable security, including guidelines and principles, are limited and those that exist are at an elementary and progressive stage. As a result, developers struggle to design security and privacy that is usable. Moreover, usable security is a relatively immature field that needs further development. Research in this field is critical, considering the fact that security and privacy tools are regarded as too complex for users to understand and apply. The need for a privacy framework in social networking environments has been emphasised, as it is seen as a possible solution to conflicting privacy issues (Hodge, 2006). Taking this into account, the purpose of the study was to develop a framework for evaluating usable security to address the usability and user experience issues that users face with regard to the security and privacy features available to them in these environments.

To develop the usable security framework it was initially required understanding the security and privacy requirements for online social networking environments from a user perspective. In addition, considering the lack of evaluation tools that can assist developers in designing usable security on applications/websites was equally important. Owing to the influence human-computer interaction has on usable security, user-centred design approaches were considered as possible evaluation tools. These are referred to as usability inspection methods and are applied to evaluate the usability of applications/websites in the field of human-computer interaction. This is achieved by identifying usability problems or violations on a user interface.

As highlighted, there is currently a paucity of knowledge and research in the literature pertaining to usable security. Hence, the focus of this study was to address this gap. This study investigated the fields of human-computer interaction, information security and usable security to determine the requirements and components that are needed to develop a conceptual framework for evaluating usable security. This framework will benefit users and developers alike and will it is anticipated prove to be a theoretical guide for developers by providing them with the ability to enhance their designs for the intended users. This will be achieved by ensuring that security and usability form a unified process that is considered in user interface design. As a result, user competencies and preferences will be acknowledged, leading to higher levels of usable security. This will, in turn, assist users in protecting their information more effectively and provide a more positive user experience. On the basis of the problems mentioned, the main research question was to determine the components of a framework to evaluate usable security. The supporting four sub-questions included, determining which usability inspection method can be adapted to evaluate usable security, which approach can be followed to develop the selected usability inspection method, how can the validity and applicability of the method and approach be illustrated, and lastly, how can the method and approach be constituted into a framework.

3 The Framework

Lethbridge and Laganiere (2005) portray the composition of a framework as process that moves between several cycles. The cycles consist of components that are connected via relationships. Together, the components and their relationships comprise one logical unit, the framework. Based on Lethbridge and Laganiere (2005) view regarding the composition of a framework, the three components of the framework to evaluate usable security in online social networks are a usable security heuristic evaluation, a three-phase process to develop heuristics for specific application domains and a validation tool. It must be noted that each phase of the process has a number of tasks. In relation to the research questions, the usable security heuristic evaluation represents the selected usability inspection method and the process to develop heuristics for specific application domains is the approach that will be used to develop the method itself. The validation tool is used to determine the validity and applicability of the method. In addition, a case study on two online health social networks was conducted to determine the validity and applicability of both the approach and the method.

As mentioned, it is required to determine the relationships between the components, before composing the final framework. In the case of the usable security framework, there are three relationships between its components. The first relationship is between the process to develop heuristics for specific application domains and the usable security heuristic evaluation. To develop the usable security heuristic evaluation the process needed to be considered and applied. The second relationship is between the validation tool and the usable security heuristic evaluation. To ensure the applicability and validity of the usable security heuristic evaluation, the validation tool had to be applied in order to assess it. The third relationship is between the process to develop heuristics for specific application domains and the validation tool. The validation tool is applied in task 2 of phase 2 in the process.

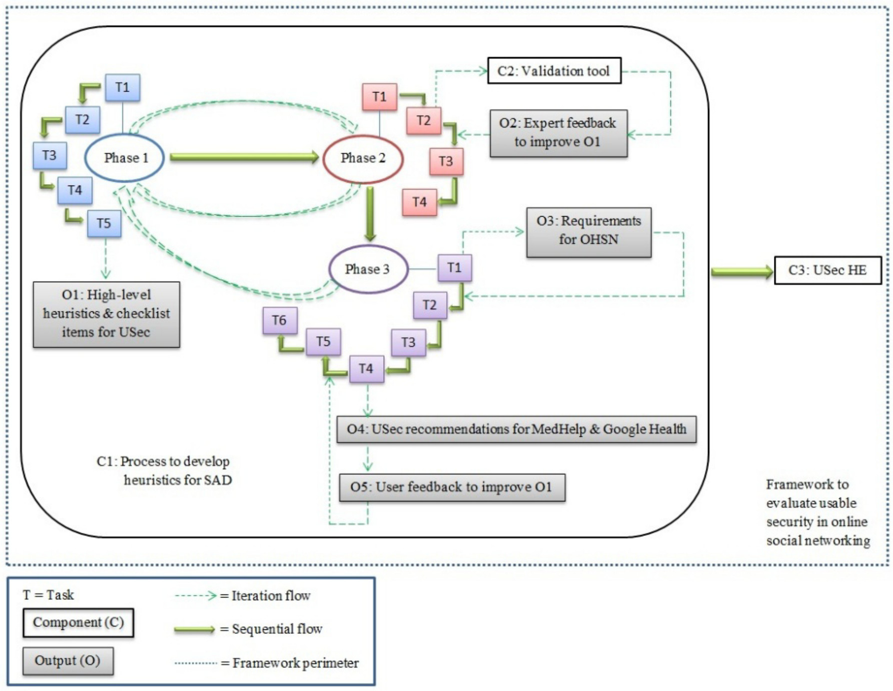
C2: Validation tool
T1
T2
T3
T4
T5
Phase 1
Phase 2
T1
T2
T3
T4
O2: Expert feedback to improve O1
O3: Requirements for OHSN
Phase 3
T1
T2
T3
T4
T5
T6
O1: High-level heuristics & checklist items for USec
C3: USec HE
O4: USec recommendations for MedHelp & Google Health
O5: User feedback to improve O1
C1: Process to develop heuristics for SAD
Framework to evaluate usable security in online social networking
T = Task
Component (C)
Output (O)
= Iteration flow
= Sequential flow
= Framework perimeter

Figure 1: Composition (components, outputs and relationships) of the framework to evaluate usable security in online social networking

The components of the framework and their relationships produce specific outputs. In terms of the framework for evaluating usable security in online social networking, the components are a process to develop heuristics for specific application domains, a validation tool and a usable security heuristic evaluation. The specific outputs that result from the components relationships are high-level heuristics and checklist items for usable security, expert feedback to improve the first output, requirements for online health social networks, usable security recommendations for MedHelp and Google Health (the websites used for the case study) and user feedback to improve the first output again.

Figure 1 illustrates the components, relationships and outputs of the usable security framework. In terms of figure 1, the following abbreviations are used: T = Task; O = Output; C = Component; OHSN = Online Health Social Networks; USec HE = Usable Security Heuristic Evaluation and SAD = Specific Application Domains. From figure 1, the three components can be identified. C1 is the process to develop heuristics for specific application domains. All outputs and C2 (the validation tool) occur within the process. C3 (the usable security heuristic evaluation) is the end result from following the entire process. Together all components, outputs and relationships form the framework to evaluate usable security in online social networks. The three components are discussed in more detail in the following sections.

3.1 Component I – Three-Phase Process to Develop Heuristics for Specific Application Domains

The main goal of usability inspection methods is to provide the best possible impact on interactive design at the lowest possible cost (Woolrych and Cockton, 2001). The application of these methods requires the continuous involvement of users in the design and evaluation phases and it must reflect the application of usability practices throughout, in order to meet their needs. In addition to user involvement, expert involvement will complement and enhance the design process. Usability inspection methods are particularly fundamental for data collection and analysis within the human-computer interaction research field. Several prevalent methods include usability evaluations, contextual inquiries and heuristic evaluations. It was stated previously that the selected method was a heuristic evaluation. Research studies show that there is often the need to develop new heuristic sets for a specific application domain, as they will yield more effective results during evaluation. Currently, there is no literature describing a systematic process that can be followed in an attempt to develop new heuristics, even though heuristic evaluations is an area in the human-computer interaction research community that has been well studied. At present, the two main themes within this space is to improve their effectiveness and to develop new heuristic sets for specialised domains (Sim, Read and Cockton, 2009). Considering that there is no systematic process to develop new heuristic sets in combination with the main themes in this research space, the three-phase process to develop heuristics for specific application domains was developed (Yeratziotis, Pottas and van Greunen, 2011a).

The process, which is represented as C1 in figure 1, initiates in phase 1, where the focus is on designing high-level heuristics for the specific application domain. Phase 1 consists of five tasks. By completing phase 1, the first outcome of the framework is achieved, represented as O1 in figure 1. It is the high-level heuristics and checklist items for usable security. The process then continues into phase 2, which consists of four tasks. The validation tool, which is the second component of the framework and discussed in the next section is applied by experts in the second task of this phase. By applying the validation tool, the second outcome of the framework is achieved, represented as O2 in figure 1. It is the feedback that experts provided to improve O1, the high-level heuristics and checklist items for usable security. Once this phase is complete the process continues to the next phase, phase 3, which focuses on applying the high-level heuristics in context. In this research, the context is the online health social networks. Phase 3 consists of six tasks and O3 is achieved by conducting the first task of this phase. It is the requirements for online health social networks. These were subsequently applied to determine the two websites that would be used in a case study, in which users would complete security and privacy tasks and then evaluate the websites with the usable security heuristic evaluation. By completing task four in this phase, O5 and O6 of the framework are achieved. They are usable security recommendations to improve the two online health social networks (Yeratziotis, Pottas and van Greunen, 2011b) and user feedback to improve the high-level heuristics and checklist items for usable security, O1.

All outputs resulting from applying the process, which is the first component of the framework and the validation tool, the second component of the framework, contribute to the third component, the final usable security heuristic evaluation, which is discussed in section 3.3. The three-phase process to develop heuristics for specific application domains is discussed in detail in (Yeratziotis et al., 2011a). This includes a discussion on each phase, its related tasks and iteration cycles that occur between the phases.

3.2 Component II – Validation Tool

The validation tool, which is represented as C2 in figure 1, is applied in task 2 of phase 2 of the process (C1). It was designed in Microsoft Excel and comprised seven sheets (or sections). These included instructions, expert biographical information, heuristics assessments, checklist items assessment, severity ratings, material assessment and a satisfaction questionnaire. The validation tool is customised for usable security; however, it can be used as a template for creating similar validation tools. The tool would be modified to evaluate the heuristics of a specific application domain for which they are being developed. The descriptions of each sheet will follow. The descriptions are based on how each sheet was used to validate the usable security heuristic evaluation.

Sheet I - instructions was used to explain the nature of a heuristic evaluation to the selected experts and how it can be used to evaluate an interface for usability violations. It then mentioned the purpose of the validation tool and the fact that it would be used to assess a new set of usable security heuristics. Additionally, specific instructions were also provided for each sheet. These were available on the actual sheet. *Sheet II - expert biographical information* was used to record the biographical details of the experts and was important to determine the level of expertise that each of the experts possessed in terms of the three fields of usable security, human-computer interaction and information security. This would help measure their comments or feedback for the modifications that are provided in the validation tool and would contribute to understanding the perspective from which they give their opinions and how they rate in terms of their level of skill in the other fields. *Sheet III - heuristics assessments* was used to assess the high-level heuristic names together with their descriptions. These form the "groups" into which relevant checklist items would be categorised. This sheet specifically addressed the importance and clarity of name and description. Experts could also provide optional comments were they felt necessary.

Sheet IV - checklist items assessment was used to assess the checklist items for each high-level usable security heuristic. These items were categorised within one of the high-level heuristics of sheet III. They are supporting and specifying high-level design issues that assist the experts to understand the application of the heuristic in context. The assessments specifically addressed the clarity, grouping and relevance of each checklist item. Measuring the clarity of the wording used for the checklist item will determine whether the terminology is clear and easy to understand or if re-wording is required in the next iteration cycle of the process (C1). Measuring the grouping for a checklist item will determine if it is well categorised under a high-level heuristic. Measuring the relevance of a checklist item will determine whether it is appropriate in identifying a security/privacy usability violation. Experts also provide a verdict on whether or not the checklist item should be included in the final usable security heuristic evaluation (C3). As with the previous sheet, experts could provide optional comments to support their ratings. To conclude their assessments, experts provided their opinions on the completeness of the set of checklist items and could also suggest additional information that should have been considered. The aim was to gain consensus among the experts to ensure that the fields of usable security, human-computer interaction and information security are considered and represented. This can be challenging at times because the fields can offer conflicting views.

Sheet V - severity ratings was used to determine the most effective ratings to be used in the usable security heuristic evaluation. Severity ratings are applied to measure the extent of usability violations in a heuristic evaluation. There are cases however where commonly used severity ratings are insufficient to measure the extent of usability violations in a specific application domain (Sim et al., 2009). In the case of the usable security heuristic evaluation, there was a need to create customised severity ratings that can be more effective in measuring the extent of usable security violations. Jakob Nielsen’s acknowledged severity ratings were insufficient to be used alone as they are based solely on a usability perspective, and consequently, they lack a security perspective. Taking into account Nielsen’s severity ratings (Nielsen, 1994), and by modifying and adapting them with the standards for security categorisation of federal information and information systems (FIPS PUB 199, 2004), it was possible to include a security perspective in them as well to compliment a usability one. The result was two different sets of usable security severity ratings that experts would assess in order to determine the most effective match for the usable security heuristic evaluation.

Sheet VI - material assessment was used to assess the material that was considered to develop the usable security heuristic evaluation. The assessment examined the usability and usable security material and the security and privacy material separately and specifically addressed the novelty and relevance of the materials. Experts could also provide optional comments were they felt necessary. *Sheet VII - user satisfaction questionnaire* was used to collect the experts overall views regarding the usable security heuristic evaluation as a tool for assessing the level of usable security in online social networking environments.

3.3 Component III – Usable Security Heuristic Evaluation

The usable security heuristic evaluation is the third component of the framework to evaluate usable security in online social networks and is represented as C3 in figure 1. A heuristic evaluation is regarded as an analytical evaluation method, which is undertaken by usability experts. The experts apply a specific set of heuristics to evaluate the usability of a user interface. This provides an immediate analysis of the website/application, which helps to correct confusing elements in the current design and leads to enhanced user experience. The method is widely used because it is an excellent method of diagnostic and perspective analysis for identifying individual problems in a short time period. Specifically, its purpose is to identify problems that are associated with the design of user interfaces. The results are dependent on the experts' broader experience with usability (Nielsen, 2005a; Straub, 2003). Several experts working independently are considered adequate and very effective for identifying usability issues. Nielsen (2005b) is of the opinion that between three to five evaluators are sufficient, as they would be able to discover an average of 75% of usability problems on the user interface.

To reiterate, by completing phase 1 of the process, high-level heuristics and checklist items for usable security (O1) were developed. By completing the entire process (C1), the final usable security heuristic evaluation (C3) is developed. The difference between O1 and C3 is that C3 includes improvements to O1, as were suggested by experts in O2 and users in O5, by applying the validation tool (C2) and conducting the case study respectively. A detailed discussion on how O1 was reached is presented in (Yeratziotis, Pottas and van Greunen, 2012). It includes a discussion on the literature that was considered, how emerging themes from the literature were transformed to high-level heuristics for usable security, how the tailored-method was applied to create the checklist items, and how these were ultimately grouped under corresponding high-level heuristics. The usable security heuristic evaluation (C3) consists of eleven heuristics and seventy checklist items that evaluate the specific application domain of usable security. Table 1 displays the heuristics (with their descriptions) and the number of checklist items within each.

#	Heuristic	Checklist Items
1	Visibility - the system should keep users informed about their security status	6
2	Revocability - the system should allow users to revoke security actions where appropriate	4
3	Clarity - the system should inform users in advance about the consequences of any security actions	4
4	Learnability - the system should ensure that security actions are easy to learn and remember	8
5	Aesthetics and Minimalist Design - the system should apply appropriate visual representation of security elements and not provide irrelevant security information	5
6	Errors - the system should provide users detailed security error messages that they can understand and act upon to recover	5
7	User Suitability - the system should provide options for users with diverse levels of skill and experience in security	4
8	User Language - the system should use plain language that users can understand with regard to security	6
9	User Assistance - the system should make security help relevant and apparent to users	6
10	Identity Signal - the system should use and display information about validated certificates	2
11	Security and Privacy - the system needs to ensure integrity, availability, confidentiality and privacy	20

Table 1: Number of checklist items for each usable security high-level heuristic

4 Practical Applicability of the Framework

The framework outlines the way in which usable security can be evaluated in the context of online social networking. The framework clarifies the components and outputs that are influenced by the relationships that exist between the components themselves and the health online social networking environment. The framework is unique and incorporates three novel components: a process, a validation tool and a heuristic evaluation. From a practical perspective, the framework consists of two reliable measuring instruments in the validation tool and the usable security heuristic evaluation. First, the process was followed to develop a heuristic evaluation for the specific application domain of usable security. The validation tool was then applied by experts in the fields of information security, human-computer interaction and usable security to validate the usable security heuristic evaluation. This was to ensure that it addressed the requirements of all fields. Once improvements were made based on the experts' feedback, participants in a case study applied the heuristic evaluation to evaluate the level of usable security on two online health social networks. The result was usable security recommendations for both online health social networks. The application of each component serves as a proof of concept, illustrating the applicability and use of the entire framework as a unit. Beyond the boundaries of the framework, the process, the usable security heuristic evaluation and the validation tool can be considered as contributions individually. The process can be applied to develop a heuristic evaluation for another specific application domain. The usable security heuristic evaluation can be used to measure the level of usable security on other websites/applications and the validation tool can be used to assess a new set of heuristics and checklist items for another specific application domain, following modifications.

5 Conclusions and the Future

When security compliments usability in online social networks, the interaction between the user and the online environment becomes beneficial. The framework to evaluate usable security in online health social networks contributes to the fields of usable security and human-computer interaction in this sense. The fact that security is a problem area for user interface design contributes to poor usable security. Consequently, developers require tools that can assist them to improve their designs in terms of usable security. Security and privacy design issues can be alleviated with the assistance of the usable security heuristic evaluation, which was used to evaluate security and privacy features of two online health social networks. Future research could be focused on applying it to evaluate another website/application (e.g. Facebook, MS Outlook, e-banking websites). Similarly, the process to develop heuristics for specific application domains was considered to develop a heuristic evaluation for the domain of usable security. Future research could be focused on applying the process to develop heuristics for another specific application domain (e.g. heuristics to evaluate the design of instructional e-learning websites for the Deaf).

6 References

FIPS PUB 199 (2004), “Federal information processing standards publication: Standards for security categorization of federal information and information systems”, Department of Commerce: USA.

Furnell, S.M., Jusoh, A. and Katsabas D. (2006), “The challenges of understanding and using security: A survey of end-users, *Computers & Security*, Vol. 25, No. 1, pp27–35.

Hodge, M.J. (2006), “The Fourth Amendment and privacy issues on the “new” Internet: Facebook.com and MySpace.com”, *Southern Illinois University Law Journal*, Vol. 31, pp95-122.

Lethbridge, T.C. and Laganiere, R. (2005), *Object-oriented software engineering: Practical software development using UML and Java*, Second edition, McGraw-Hill-Education, Berkshire, England, ISBN: 9780077109080.

Nielsen, J. (1994), “Heuristic evaluation”, in Nielsen J. and Mack, R.L. (Ed), *Usability inspection methods*, John Wiley & Sons, New York, ISBN: 0-471-01877-5.

Nielsen, J. (2005a), “Useit.com: Heuristic evaluation”, http://www.useit.com/papers/heuristic/, (Accessed 10 October 2010).

Nielsen, J. (2005b), “Useit.com: How to conduct a heuristic evaluation”, http://www.useit.com/papers/heuristic/heuristic_evaluation.html, (Accessed October 10 2010).

Sasse, M. and Flechais, I. (2005), “Usable Security Why do we need it? How do we get it?”, in Cranor, L.F. and Garfinkel, S. (Ed), *Security and Usability: Designing Secure Systems That People Can Use*, O’ Reilly Media Inc., Sebastopol, CA. ISBN: 0-596-00827-9.

Sim, G., Read, J.C. and Cockton, G. (2009), “Evidence based design of heuristics for computer assisted assessment”, in *INTERACT '09 proceedings of the 12th IFIP TC 13 International Conference on Human-Computer Interaction: Part I*, Uppsala, Sweden.

Whitten, A. and Tygar, J.D. (2005), "Why Johnny can't encrypt: A usability evaluation of PGP 5.0", in Cranor, L.F. and Garfinkel, S. (Ed), *Security and Usability: Designing Secure Systems That People Can Use*, O' Reilly Media Inc., Sebastopol, CA. ISBN: 0-596-00827-9.

Woolrych, A. and Cockton, G. (2001), "Why and when five test users aren't enough", in Vanderdonckt, J., Blandford, A. and Derycke, A. (Ed), in *proceedings of IHM-HCI 2001*, Toulouse, France, Vol. 2, pp105–108.

Yee, K. (2002), "User interaction design for secure systems", in *proceedings of the 4th International Conference on Information and Communications Security, 2002 (ICICS' 02)*, Springer-Verlag, London, UK, pp 278–290.

Yeratziotis, A., Pottas, D. and van Greunen, D. (2011a), "A Three-Phase Process to Develop Heuristics", in *proceedings of the 13th ZA-WWW conference*, 14–16 September 2011, Johannesburg, South Africa.

Yeratziotis, A., Pottas, D. and van Greunen, D. (2011b), "Recommendations for Usable Security in Online Health Social Networks", in *proceedings of the joint conference of the 2011 6th International Conference on Pervasive Computing and Application (ICPCA) and the 2011 3rd International Symposium of Web Society (SWS)*, 26-28 October 2011, Port Elizabeth, South Africa.

Yeratziotis, A., Pottas, D. and van Greunen, D. (2012), "A usable security heuristic evaluation for the online health social networking paradigm", *International Journal of Human-Computer Interaction*, Vol. 29, No. 3.