Identifying usability activities integrated into the planning phase of the Secure Software Development Cycle through a systematic review

Juan R. Lipán Mella[1], Yenny A. Méndez A. [1]

[1]Universidad Mayor

juan.lipan@mayor.cl, yenny.mendez@umayor.cl

Abstract. Security and usability represent essential aspects to consider in the process of the development of technological solutions. However, there is evidence of a great separation of these aspects that requires special attention. Before generating research on usable security issues, this article presents a systematic review whose purpose was to identify related works that propose usability activities in the planning phase of the life cycle of secure software development.

Keywords: Usable security, Security, Secure Software Design.

1. Introduction

Requirements Engineering corresponds to the branch of Software Engineering that deals with documenting information systems'needs and establishing their functionalities and limitations [1]. Therefore, it is essential to establish usable and safe requirements, allowing us to generate systems that are more understandable by the user, and in this way, avoid that people commit on errors in their use or that they may be vulnerable. Since usable security is a poorly understood and addressed topic, a review of the existing literature was required. The following work presents a systematic review to learn about related works on usability activities, in the early stages of software development, as part of a secure software development methodology.

The next section presents the related issue. Next, section 2 presents the conceptual basis on which this review is supported. Section 3 presents information on the process that was carried out to carry out the systematic review. Section 4 Information on the results obtained, and finally, in Section V, conclusions of the work carried out are presented.

1.1 The problem

Every day, modern information systems (IS) grow in size and become more complex, making their monitoring and security considerably more difficult. Organizations that implement these information systems to manage day-to-day operations are spending billions of dollars on security technologies such as firewalls, encryption software, and more to ensure their data security. Most of the time, organizations and information stakeholders forget to address issues related to the security chain's weakest link: human or usability concerns [2].

Requirements are a nexus between HCI and information security, however, it is often confused about the security requirements, how they should be expressed, and how they should best be obtained and analyzed. Techniques and frameworks are lacking to address usability, requirements, and security concerns jointly. Existing tool support for usability engineering is weak, and existing tool support for security engineering suffers from scalability when integrated with complementary approaches [1].

Over the years, different security mechanisms have been incorporated to achieve these goals, such as authentication and authorization. However, the rate of attacks on computer systems increases, and the situation can be critical, especially for large systems. Because of this, many researchers pay attention to the field of software security to produce a high-security system [3].

There are significant financial and reputational losses related to security issues that could have been addressed during requirements specification. While various approaches have been proposed for specifying security requirements, there is a definite lack of support during testing [4].

To investigate and contribute to the integration of usability activities in the requirements analysis phase in a secure development methodology, it begins with the search for literature through a systematic review, supported by the methodology proposed by Kitchenham and Charters [5].

2 Definitions

Definitions that are considered necessary to recognize before presenting the results of the systematic review are presented below:

2.1 Usability

The International Standard Organization (ISO) defines usability "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use [6].

2.2 Defining Usability for Security

“Security software is usable if people who are expected to use it: are reliably made aware of the security tasks they need to perform; are able to figure out how to successfully perform those tasks; don’t make dangerous errors; are sufficiently comfortable with the interface to continue using it” [7].

2.3 Software engineering

Software engineering is an engineering discipline concerned with all aspects of software production, from the early stages of system specification to the system's maintenance after it is put into operation [8].

2.4 Requirements

The requirements specify what the system should do (its functions) and its essential and desirable properties. The main objective of capturing the requirements is to understand what customers and users expect the system to do. A requirement expresses the purpose of the system without considering how it will be implemented. In other words, requirements identify the what of the system, while the design establishes the how of the system [9].

3 Systematic review

The literature search was supported by the guidelines for conducting systematic literature reviews in software engineering [5]. Each of the steps is described below.

3.1 Research question

The question that started the literature review was: *What usability activities have been proposed to be integrated into the methodology for the development of secure software in the requirements analysis stage*?

3.1 Key words

The key words used in the searches for related works were selected; these words were: usability, methodology, development, and secure software, to obtain the most significant documentation search, synonyms, and terms similar to the critical terms. In this regard, Table 1 shows the list of words in the English and Spanish search languages.

Table 1. Key terms in Spanish and English.

Key words	Spanish	English
Usabilidad	Usable	Usability, Usable
Metodología	Proceso, Método	Methodology, Methods. Model, Framework
Desarrollo	Programación	Development
Software Seguro		"Software Security", "Software Secure", "Application Security", "Application Secure"

3.2 Databases

The databases selected to carry out the systematic review are presented in Table 2. Articles, conferences, books, book chapters that are published, among others, which are considered to be timely sources of information for searching for information.

Tabla 2. Selected Databases

Database	Link
IEEE Xplore	https://ieeexplore.ieee.org/
ACM Digital Library	https://dl.acm.org/
Web of Science	https://webofknowledge.com
Scopus	https://www.scopus.com/
Springer	https://www.springer.com

3.3 Inclusion and exclusion criteria

The inclusion and exclusion criteria considered in the systematic review are presented below:

Inclusion criteria

1. Documents related to the initial phase of the software development process.
2. Documents that are related to usability activities with the initial phase of the secure software development process.
3. The searches will be in languages: Spanish and English.
4. Only articles published after 2009 will be considered.

Exclusion criteria

1. Articles that do not have full access are not considered.
2. Terms and synonyms other than those defined in the systematic review process are not considered.
3. Documents other than: Articles (Conferences and Journals) and Magazines (Magazines) are not considered.
4. Searches other than metadata are not considered: Title, Abstract and Author's Keywords.

3.4 Query search

Based on the previously established terms and the purpose of the systematic review, the following search strings were established:

Tabla 3. Query search in Spanish and English.

Language	Query search
Spanish	((Usab*) AND (Metodo* OR Proceso) AND (Desarrollo OR Programación) AND ("Software Seguro")) AND (AÑO >= 2009)
English	((Usab*) AND (Method* OR Model OR Framework) AND (Development) AND (("Software Secur*") OR ("Application Secur*"))) AND (AÑO >= 2009)

3.5 Search and revision

The search procedure is carried out by accessing the five defined databases (IEE Xplore, ACM Digital Library, and Web of Science, Scopus, and Springer), defining an advanced search string with established keywords. Once the results were obtained, they were organized in a spreadsheet, assigning a number to each article. From the search, 44 articles were obtained, distributed in the different databases (see Fig. 1).

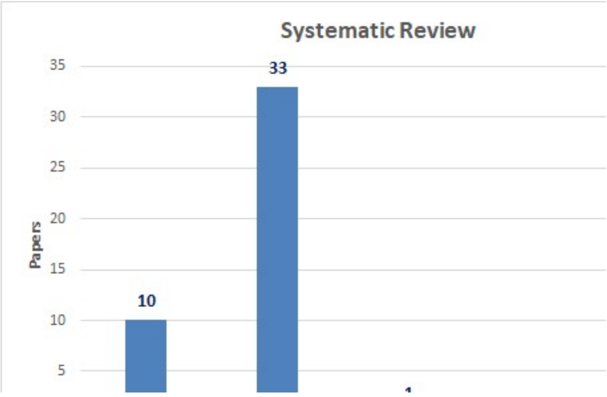

Fig. 1. Relationship between articles found and selected databases

The selection of papers was supported by two search filters that are detailed below:

First filter results

A first review of the documents is carried out, reviewing the documents' abstracts and considering the first two inclusion criteria.

1. Documents related to the initial phase of the software development process.

2. Documents related to usability activities in the initial phase of the software development process.

Table 4 presents information on the number of articles included and articles excluded from the first filter.

Table 4. First filter results**.**

Databases	Number of items	Included	Excluded
IEEE Xplore	10	5	5
ACM Digital Library	33	9	24
Web of science	1	1	0
Scopus	0	0	0
Springer	0	0	0
Total	44	15	29

Second filter results

Introductions and conclusions of the 15 articles resulting from the first filter were reviewed, and the first two inclusion criteria were considered. Table 5 shows the list of articles included and articles excluded from the second filter.

Table 5. Second filter results**.**

Databases	Number of items	Included	Excluded
IEEE Xplore	5	1	4
ACM Digital Library	9	4	5
Web of science	1	1	0
Total	15	6	9

The second filter results in 6 articles, which are reviewed in their entirety. From this review, 3 articles have been selected that answer the research question. The relationship between the number of articles and the year of publication is presented in Fig 2.

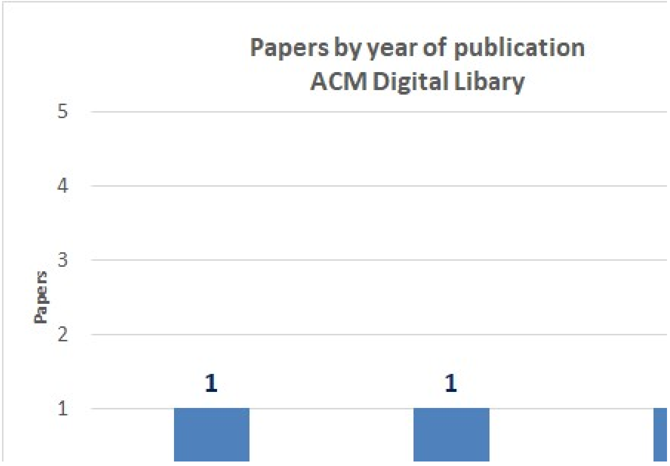

Fig. 2. Selected articles to a full review

3.5 Results

It is important to note that no articles were found in Spanish; all articles were accessed, the articles were written entirely in English, and no repeated articles were found.

About selected articles
The most critical points of the 3 articles that are part of the research process, which will allow us to answer the systematic review question, are described below.

The article "Closing the Feedback Loop Between UX Design, Software Development, Security Engineering, and Operations" [10], proposes an adaptation of the Secure Development Lifecycle (SDL) and the DevSecOps model for agile development. Usability (UX) designers and researchers are included in the Technology Development Lifecycle.

The paper “Developer-centered security and the symmetry of ignorance” [11], presents a proposal for changes in the culture of developments, processes, and technology to address developer-centric security.

The paper “Secure and Usable Requirements Engineering” [12], proposes the Safe Usable Requirements Engineering (SURE) technique, which aims to increase the usability of software requirements in their development stages. It serves as a support to elicit, analyze and specify security requirements and documents in the early stages of development, misuse processes, and possible threats to the system. It seeks to increase the usability of the specified security requirements to be traceable in development, and usability is increased.

4 Conclusions

The systematic review made it possible to identify the existing literature related to "usability activities have been proposed to integrate into the methodology for the development of secure software in the requirements analysis stage." It is evidenced that there is not enough information in the selected databases on related research. Forty-four articles were found in the five databases used, selecting only 3 that directly contribute to answer the question that gave rise to the systematic review.

The selected articles describe usability and security activities that can be included in the initial phases of software development, which could contribute to generate solutions that are easier to use and more secure, avoiding exposing the user to risks or misuse of the software.

This systematic review is a basis for developing other research on issues related to usability activities in the requirements gathering stages, as part of a secure development methodology.

References

1. S. Faily, "Usable and Secure Software Design: The State-of-the-Art," in *Designing Usable and Secure Software with IRIS and CAIRIS*, 2018, pp. 9–53.
2. B. Naqvi and A. Seffah, "A Methodology for Aligning Usability and Security in Systems and Services," *Proc. - 2018 3rd Int. Conf. Inf. Syst. Eng. ICISE 2018*, pp. 61–66, 2019, doi: 10.1109/ICISE.2018.00019.
3. O. M.Surakhi, A. Hudaib, M. AlShraideh, and M. Khanafseh, "A Survey on Design Methods for Secure Software Development," *Int. J. Comput. Technol.*, vol. 16, no. 7, pp. 7047–7064, 2017, doi: 10.24297/ijct.v16i7.6467.
4. J. Romero-Mariona, H. Ziv, and D. Richardson, "ASSURE: Automated support for secure and Usable Requirements Engineering," *ISSTA'10 - Proc. 2010 Int. Symp. Softw. Test. Anal.*, no. Mc, pp. 279–282, 2010, doi: 10.1145/1831708.1831744.
5. Kitchenham, "Guidelines for performing systematic literature reviews in software engineering," *Tech. report, Ver. 2.3 EBSE Tech. Report. EBSE*, 2007.
6. International Organization for Standardization, "ISO 9241-11:2018(en) Ergonomics of human-system interaction", International Organization for Standardization," 2018.
7. A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt," *USENIX Secur. Symp.*, pp. 679–702, 1999.
8. I. Sommerville, *Ingeniería de Software, Novena edición*. 2017.
9. M. Gómez, *Notas Del Curso: Análisis de Requerimientos*. 2011.
10. J. Nguyen and M. Dupuis, "Closing the Feedback Loop Between UX Design, Software Development, Security Engineering, and Operations," in *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, 2019, pp. 93–98, doi: 10.1145/3349266.3351420.

11. O. Pieczul, S. Foley, and M. E. Zurko, “Developer-Centered Security and the Symmetry of Ignorance,” in *Proceedings of the 2017 New Security Paradigms Workshop*, 2017, pp. 46–56, doi: 10.1145/3171533.3171539.
12. J. Romero-Mariona, “Secure and Usable Requirements Engineering,” in *Proceedings of the 2009 IEEE/ACM International Conference on Automated Software Engineering*, 2009, pp. 703–706, doi: 10.1109/ASE.2009.81.