Concurrent Consideration of Technical and Human Aspects in Security Requirements Engineering

Damjan Fujs
University of Ljubljana, Faculty of Computer and Information Science, Ljubljana, Slovenia
E-mail: damjan.fujs@fri.uni-lj.si

Thesis summary

Keywords: information security, software feature, training

Received: March 18, 2024

This article is an extended abstract of the doctoral dissertation entitled "Tailoring security-related software and training requirements to users based on their categorization" [1]. Security has traditionally been ensured by technical solutions in the concluding stages of software development. The fact that security is considered an additional function means that a vulnerability is fixed with security patches as soon as it occurs. However, the importance of human factors is increasingly being recognized, as technical solutions alone are not enough to close security gaps. In order to address this shortcoming, we proposed an approach that simultaneously addresses technical as well as human aspects - already in the initial stages of software development.

Povzetek: Predstavljena je doktorska disertacija z naslovom »Prilagajanje z varnostjo povezanih zahtev za programsko opremo in usposabljanja uporabnikov na podlagi njihove kategorizacije«.

1 Introduction

The number of cyber security threats is increasing. Not only the number of threats, but also in terms of their impact and severity of consequences [4]. Despite the fact that established technical information security mechanisms can be effective, human factors remain one of the key challenges in ensuring information security because people are the weakest link in information security [3].

The main objective of the doctoral dissertation was to investigate how the technical and human aspects of information security can be addressed simultaneously to improve overall information security.

2 Methods

Our approach consists of two main phases and three steps. In the *first* phase, we developed a novel approach for tailoring information security training requirements (iSTR) based on end user categorization according to their different levels of information security performance. In the *second* phase, we developed an approach for balancing information security software requirements (iSSR) and iSTR (See Figure 1). The overall approach is based on existing studies in the field of software requirements engineering, human aspects of information security (user groups), information security standards and security-related software requirements and training.

To test the proposed approach, we conducted an experiment (our main research method) among experienced information system professionals from the wider field of software development (N=128). For the needs of the experiment, we prepared supporting artefacts in which we introduced the basic concepts, the research process and additional explanations to the participants. Participants were randomly assigned to an experimental (N=66) or control group (N=62).

3 Results

The main result shows a clear difference between the two groups in favour of the experimental group. The difference between the two groups is statistically significant (p-value < 0.001). Assessments of evaluators (i.e., experienced experts in the field of information security) show that the requirements created by the experimental group were better than the requirements created by the control group.

In addition, we conducted a post-hoc survey in which we asked the participants of the experiment about three indicators: complexity, compatibility and usefulness. The results are statistically significant (p-value < 0.001) for the usefulness. These results indicate that the participants in the experimental group did not perceive our approach as significantly more complex or less consistent with their knowledge. In addition, participants in the experimental group found our approach significantly more useful than the approach they used in the control group.

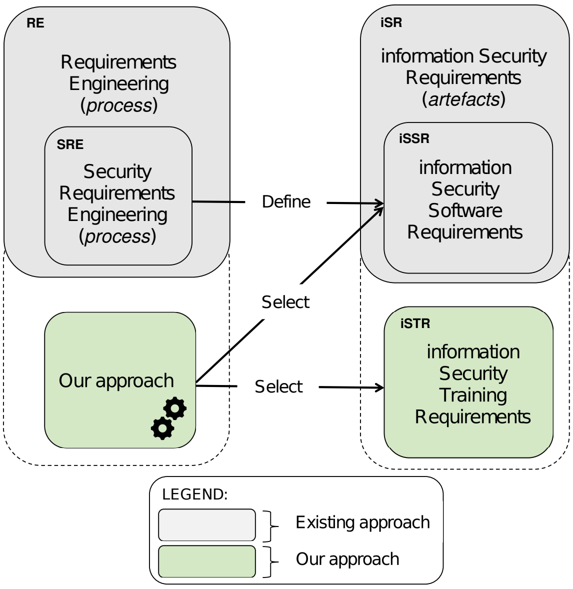
RE
Requirements Engineering (*process*)
SRE
Security Requirements Engineering (*process*)
Define
iSR
information Security Requirements (*artefacts*)
iSSR
information Security Software Requirements
Select
Our approach
Select
iSTR
information Security Training Requirements
LEGEND:
Existing approach
Our approach

Figure 1: Main research concepts and their relationship. The green color shows our contribution (i.e. our approach that enables balancing iSSR and iSTR), while the grey color represents elements that are already established in the literature. Figure modified from Fujs [1].

4 Conclusion

The following contributions to science in the field of computer and information science are presented in the doctoral dissertation [1]: 1. A novel approach for identifying information security-related training requirements based on end-user categorization of their information security performance (security-related knowledge, attitudes and behaviors). 2. A novel approach that allows iSSR and iSTR to be considered simultaneously based on end user categorization.

Acknowledgements

The author would like to thank the mentors (Damjan Vavpotič and Simon Vrhovec) and committee (Denis Trček, Igor Bernik, Steffen Wendzel and Tomaž Curk). Many thanks to President of the World Federation of Scientists, Prof Antonino Zichichi, for granting a scholarship to support the completion of the author's doctoral studies.

References

[1] Fujs, D. (2024). *Tailoring security-related software and training requirements to users based on their categorization* [Doctoral dissertation]. Repository of the University of Ljubljana.

[2] Fujs, D., Vrhovec, S., & Vavpotič, D. (2023). Balancing software and training requirements for information security. *Computers & security*, 134, 103467. https://doi.org/10.1016/j.cose.2023.103467

[3] Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & Security, 88, 101640. https://doi.org/10.1016/j.cose.2019.101640

[4] European Union Agency for Cybersecurity, Svetozarov Naydenov, R., Malatras, A., Lella, I., Theocharidou, M., Ciobanu, C., Tsekmezoglou, E. (2022). ENISA threat landscape 2022. https://doi.org/10.2824/764318