Model Comprehension for Security Risk Assessment: An Empirical Comparison of Tabular vs. Graphical Representations

Katsiaryna Labunets[1] Fabio Massacci[2] Federica Paci[3] Sabrina Marczak[4] Flávio Moreira de Oliveira[4]

[1]Delft University of Technology, NL [2]University of Trento, IT [3]University of Southampton, UK [4] Pontifícia Universidade Catòlica do Rio Grande do Sul, BR

ABSTRACT

Context: Tabular and graphical representations are used to communicate security risk assessments for IT systems. However, there is no consensus on which type of representation better supports the comprehension of risks (such as the relationships between threats, vulnerabilities and security controls). Vessey's cognitive fit theory predicts that graphs should be better because they capture spatial relationships. **Method:** We report the results of two studies performed in two countries with 69 and 83 participants respectively, in which we assessed the effectiveness of tabular and graphical representations concerning the extraction of correct information about security risks. **Results:** Participants who applied tabular risk models gave more precise and complete answers to the comprehension questions when requested to find simple and complex information about threats, vulnerabilities, or other elements of the risk models. **Conclusions:** Our findings can be explained by Vessey's cognitive fit theory as tabular models implicitly capture elementary linear spatial relationships. **Interest for ICSE:** It is almost taken for granted in Software Engineering that graphical-, diagram-based models are "the" way to go (e.g., the SE Body of Knowledge [3]). This paper provides some experimental-based doubts that this might not always be the case. It will provide an interesting debate that might ripple to traditional requirements and design notations outside security.

KEYWORDS

Empirical Study, Security Risk Assessment, Risk Modeling, Comprehensibility, Cognitive Fit

ACM Reference Format:
Katsiaryna Labunets[1] Fabio Massacci[2] Federica Paci[3] Sabrina Marczak[4] Flávio Moreira de Oliveira[4]. 2018. Model Comprehension for Security Risk Assessment: An Empirical Comparison of Tabular vs. Graphical Representations. In *ICSE '18: 40th International Conference on Software Engineering, May 27-June 3, 2018, Gothenburg, Sweden.* ACM, New York, NY, USA, Article 4, 1 page. https://doi.org/10.1145/3180155.3182511

1 SUMMARY OF FINDINGS

This work aims to study which risk model representation is more comprehensible for stakeholders in extracting correct information about security risks. Thus, our research questions are:

RQ1 Which risk modeling notation, tabular or graphical, is more effective in extracting correct information about security risks?

RQ2 What is the effect of task complexity on participants' actual comprehension of information presented in risk models?

To answer the research questions, we design special comprehensibility tasks to measure the participant's ability to extract correct information about security risks using tabular and graphical models. We considered comprehension questions of different complexity (simple vs. complex) in line with Wood's theory of task complexity [4]. See Labunets et al. [1] for more details.

We selected scenarios from the healthcare and online banking domains, modeled the security risks of the scenario in the two notations, and asked the participants to answer several questions of different complexity. By using precision and recall of participants' responses, we compared the effect of the modeling notation on the comprehensibility of the risk models. The results of our study show that tabular risk models are more effective than the graphical ones w.r.t. simple comprehension tasks and in some cases are more effective for complex ones.

2 A NATURAL FOLLOW-UP QUESTION

One of the reviewers of the paper asked whether our "tasks accidentally favor the tabular representation (beyond any advantage it might have by itself)?" To address this issue, we conducted an experiment with professionals to study if the availability of textual labels and terse UML-style notation could improve comprehensibility.

In [2] we reported the results of an online comprehensibility experiment involving 61 professionals with an average of 9 years of working experience. We compared the ability to comprehend security risk assessments represented in tabular, UML-style with textual labels, and iconic graphical modeling notations. The experiment confirmed previous findings: the tabular notation is still the most comprehensible in both recall and precision. However, the presence of textual labels does improve the precision and recall of participants over iconic graphical models.

REFERENCES

[1] Katsiaryna Labunets, Fabio Massacci, Federica Paci, Sabrina Marczak, and Flávio Moreira de Oliveira. 2017. Model comprehension for security risk assessment: an empirical comparison of tabular vs. graphical representations. *Empir. Soft. Eng.* 22, 6 (2017), 3017–3056.

[2] Katsiaryna Labunets, Fabio Massacci, and Alessandra Tedeschi. 2017. Graphical vs. Tabular Notations for Risk Models: On the Role of Textual Labels and Complexity. In *Proc. of the 11th ACM/IEEE Int. Symp. on Empirical Software Eng. and Measurement.* IEEE, 267–276.

[3] Joint Task Force on Computing Curricula. 2015. *Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering.* Technical Report. Available at http://www.acm.org/binaries/content/assets/education/se2014.pdf.

[4] Robert E Wood. 1986. Task complexity: Definition of the construct. *Organ. Behav. Hum. Dec.* 37, 1 (1986), 60–82.

ICSE '18, May 27-June 3, 2018, Gothenburg, Sweden

ACM ISBN 978-1-4503-5638-1/18/05.
https://doi.org/10.1145/3180155.3182511