POSTER: A comparative analysis of manual methods for analyzing security requirements in regulatory documents

Sarah Elder
North Carolina State University
seelder@ncsu.edu

Anna Mattapallil
North Carolina State University

Laurie Williams
North Carolina State University
williams@csc.ncsu.edu

ABSTRACT

Developing security requirements that are compliant with security regulations is key for developing secure software systems. Statements within regulatory documents are frequently overlapping, both within and between documents. Approaches to identifying and address this overlap have been developed in academia and industry. However, these approaches have largely been evaluated in isolation. *The goal of this research is to assist analysts in selecting an appropriate approach for developing security requirements from regulatory documents by comparing the output of approaches from academic publications with similar outputs from industry.* Our initial results show that there is wide variance in how information is aggregated from security regulations at the requirement level.

CCS CONCEPTS

• **Security and privacy → Software security engineering**; • **Software and its engineering →** *Requirements analysis*;

KEYWORDS

security requirements, regulatory documents

ACM Reference format:
Sarah Elder, Anna Mattapallil, and Laurie Williams. 2018. POSTER: A comparative analysis of manual methods for analyzing security requirements in regulatory documents. In *Proceedings of Hot Topics in the Science of Security Symposium, Raleigh, NC USA, April 2018 (HoTSoS'18),* 1 pages.
https://doi.org/10.475/123_4

1 INTRODUCTION

For many projects, determining what security features are feasible for inclusion in the system begins with what security regulations they must comply with [1]. Consequently, these regulations are a useful starting point for developing security requirements for software systems. We use the term "regulations" loosely here to include documents created by state-actors, corporations, or other groups; for example legislation, standards, privacy policies, and other documents.

Extracting information from regulatory documents to develop compliant requirements specifications has many approaches, both in industry and in the academic literature. However, these approaches are largely evaluated in isolation with little empirical comparison between approaches. In this research, we identify the relevant methodologies for extracting security requirements from regulations. We categorize them using common classifications such as the level of formality [7], amount of automation, stakeholders/end-users identified [6], and study design[4, 5]. We then apply several approaches to evaluate them based on guidelines such as the amount of interpretation necessary to apply the model [3], the effort involved in applying the model, and the extent to which the resulting requirements are verifiable and traceable [2]. Unlike most of the existing literature, we do not look at consistency and completeness as these concepts are difficult to define in the security domain.

2 POSTER CONTENT

The poster will include a high-level overview of the literature reviewed, as well as results from our ongoing manual application of the methodologies to various U.S. regulatory documents. Our findings to date indicate that while the methodologies do provide some standardization of results between individuals applying the methodologies, there is still significant interpretation involved. Application of the manual methodologies is time-consuming for most security regulations, which tend to be longer than the examples described in the literature.

REFERENCES

[1] Travis Breaux and Annie Antón. 2008. Analyzing regulatory rules for privacy and security requirements. *IEEE transactions on software engineering* 34, 1 (2008), 5–20.
[2] IEC ISO. 2011. IEEE. 29148: 2011-Systems and software engineering-Requirements engineering. (2011).
[3] Ivan Jureta, Travis Breaux, Alberto Siena, and David Gordon. 2013. Toward benchmarks to assess advancement in legal requirements modeling. In *Requirements Engineering and Law (RELAW), 2013 Sixth International Workshop on.* IEEE, 25–33.
[4] Barbara Ann Kitchenham, David Budgen, and Pearl Brereton. 2015. *Evidence-based software engineering and systematic reviews.* Vol. 4. CRC Press.
[5] Laurie Breaux Travis D. Maria Riaz, Williams and Jianwei Niu. 2012. *On the design of empirical studies to evaluate software patterns: A survey.* Technical Report. North Carolina State University. Dept. of Computer Science.
[6] Nicolas Sannier, Mehrdad Sabetzadeh, and Lionel C Briand. 2017. From RELAW Research to Practice: Reflections on an Ongoing Technology Transfer Project. In *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW).* IEEE, 204–208.
[7] Axel Van Lamsweerde. 2001. Building formal requirements models for reliable software. In *International Conference on Reliable Software Technologies.* Springer, 1–20.

HoTSoS'18, April 2018, Raleigh, NC USA

ACM ISBN 123-4567-24-567/08/06.
https://doi.org/10.475/123_4