Web-based collaborative security requirements elicitation

Dan Ionita* and Roel Wieringa

University of Twente, Services, Cybersecurity and Safety group,
Drienerlolaan 5, 7522 NB Enschede, The Netherlands
{d.ionita,r.j.wieringa}@utwente.nl
http://scs.ewi.utwente.nl/

Abstract. This empirical study aims at evaluating a structured but informal security requirements engineering method supported by a collaborative Web-based tool. The method allows stakeholders to contribute to the risk analysis and security requirements of elicitation of a software or system in a structured manner that allows traceability between vulnerabilities and mitigations. The tool's collaborative and distributed workflow promotes higher levels of participation for busy practitioners with a minimum investment of time.
REFSQ participants will have the opportunity to test our new platform, and to provide feedback. The experiment revolves around a fictitious scenario. Interested individuals can connect to our server at any time and all results will be publicly available. The tool is available as Open Source software and will later be made available as virtual machine too.

Keywords: security requirements, real-time, collaborative, Web-based

1 Introduction

1.1 Research problem

With the steady rise in complexity, pervasiveness and interconnectivity of software and software-enabled devices, demand for trustworthy software is increasing [3]. Systematically addressing security considerations as early as the design stages has been shown to increase the overall quality of software [1].

However, elicitation of security requirements involves identifying and understanding the potential vulnerabilities and risks that the software might encounter throughout its lifecycle [3]. Such risk analyses commonly involves multiple stakeholders, especially when decisions with regard to the cost-effective mitigation, transfer or acceptance of risks have to be made [5]. These experts are expensive and have little time. To achieve good results, they usually meet in several sessions of several hours each, which is hard to plan due to the busy schedules.

* With support from the Web Symphony team, especially Baltuta Andrei and Emanuel Sandu

Security requirements elicitation requires assessment of security risks and of trade-offs among risk mitigations. This requires the maintenance of traceability relations among risks, vulnerabilities, mitigations, and security goals, which makes the process even more time-consuming.

Our goal is to provide practitioners with a light-weight, tool-based methodology that allows for conducting informal, qualitative risk analyses of software and systems in a collaborative way, such as to support traceable security requirements elicitation at early stages of development.

2 Previous work

We previously experimented with both formal logic-based frameworks ([4]) and informal argumentation structures ([2]) as ways of supporting systematic security requirements elicitation sessions. While too strict formalism can add unnecessary overhead, argumentation-based sessions provide minimal structure to both the assessment and its results, thus increasing both trace-ability the trace-ability and re-usability of results.

Based on previous work, we developed two software tools which employ a simplified argumentation structure, while providing an intuitive, usable interface. One is a desktop tool, meant to be used as for centralized bookkeeping during brainstorming meetings where security risks and requirements are being discussed. The other, called ArgueSecure, is a collaborative, browser-based version which allows for distributed risk analysis and security requirements elicitation sessions. While the desktop tool is aimed at providing structure to brainstorming sessions, ArgueSecure hopes to increase participation of high-level stakeholders by allowing users to contribute from anywhere, at any time, using any Web-enabled device. The browser-based tool, ArgueSecure, allows distributed and asynchronous collaboration of security experts and maintains the relation between risks and mitigations. Our research questions concern this tool.

3 Research questions for the Live Study

Q1 Does a collaborative Web-based tool encourage high-level stakeholders to participate in the security requirements elicitation process?
Q2 Is the tool perceived as useful without overburdening the analysts?

4 Research design

4.1 Type of study

As the tool to be evaluated is entirely Web-based, no plenary session is needed. Interested participants may take part at any time during the conference, from any Internet-enabled device and can provide feedback via an online questionnaire. A link to the tool and on-line questionnaire will be distributed in the conference bag. The questionnaire will ask participants for their background in risk assessment.

4.2 Population of interest

All stakeholders of software engineering projects.

4.3 Participants

No particular participant profile is required, although basic demographics will be collected for statistical purposes. As the research is purely, qualitative, there is no minimum required number of participants. However, we hope to gather meaningful feedback from at least 30 participants in order to draw well-founded and diverse conclusions. Participants may interact anonymously with each other via the platform, and gain insight into the perceived risks of participating in a conference. There is no required time investment, anything between a few minutes and a few hours is possible.

4.4 Treatment

Interested participants will be provided with a fictional scenario: a disgruntled researcher wants to sabotage the REFSQ conference. They will then be asked to identify and structure the potential risks that the conference and its participants might be facing. Furthermore, they will be asked to suggest countermeasures or controls to mitigate these risks.

Participants will receive two links: the first allows them to log into onto a private deployment of the ArgueSecure Risk Assessment platform and contribute to the collaborative risk assessment or create private assessments; the second will contain an online questionnaire asking them to evaluate their experience. The two pages will be accessible for the duration of the conference.

4.5 Measurement design

The Web–based collaborative security requirements elicitation methodology and tool will be evaluated on its utility and usability by means of an online questionnaire asking users to rank the tool based on the following indicators:

- Utility
  - Perceived Utility: How suitable do users think the ArgueSecure tool was for brainstorming about risks?
  - Effectiveness: Did the usage of the tool provide meaningful results (i.e. structured, trace-able security requirements)?
- Usability
  - Learnability: How easy was it to accomplish basic tasks on first use?
  - Efficiency: After understanding the basic functionality, how quickly can one perform desired tasks?
  - Memorability: If a user logged in to the ArgueSecure platform more than once, did subsequent usage require them to re-establish proficiency?
  - Errors: How many errors do users make, how severe are these errors, and how easily do these errors impact the result?
  - Satisfaction: How pleasant is it to use the tool? What could be improved?

4.6 Inference design

The measurements described above will be used to evaluate the usability and utility of the software tool, which in turn will be used to draw conclusions with regard to the validity of the proposed methodology, as well as future work.

The resulting risk landscape will be evaluated on its quality, completeness, and relevance to draw conclusions about the applicability of collaborative, qualitative argument-based risk analysis for the elicitation of security requirements.

4.7 Threats to validity

Some participants might spend more time than others of time experimenting with the tool or might have previous risk assessment experience, thus skewing the results. We mitigate this by asking how long a participant interacted with the tool and about his experience in risk assessment.

4.8 Ethical considerations

All participation is optional and participants can drop out at any time or refuse to participate at all without any consequences and without providing an explanation. Inform consent, including full disclosure of research goals and measurements will be assured via the landing page. All participation is anonymous: except for randomly generated usernames, no user-specific data whatsoever is captured or stored. The ArgueSecure platform is hosted on a private, secure server, located in The Netherlands. No plug-ins, downloads.

4.9 Practical considerations

Promotion of the study Via fliers containing a link to the ArgueSecure platform and one to the anonymous questionnaire as URLs and QR codes, as well as a randomly generated account. These could be provided at registration.

Equipment and infrastructure Participants can use any Web-enabled device.

References

1. El-Hadary, H., El-Kassas, S.: Capturing security requirements for software systems. Journal of Advanced Research 5(4), 463 – 472 (2014)
2. Ionita, D., Bullee, J.W., Wieringa, R.: Argumentation-based security requirements elicitation: The next round. In: Evolving Security and Privacy Requirements Engineering (ESPRE), 2014 IEEE 1st Workshop on. pp. 7–12 (Aug 2014)
3. Management Association, I.R.: Standards and standardization: Concepts, methodologies, tools, and applications: Concepts, methodologies, tools, and applications. chap. Chapter 22: Software Security Engineering, pp. 459–494. IGI Global (2015)
4. Prakken, H., Ionita, D., Wieringa, R.: Risk assessment as an argumentation game. In: Leite, J., Son, T.C., Torroni, P., van der Torre, L., Woltran, S. (eds.) CLIMA. Lecture Notes in Computer Science, vol. 8143, pp. 357–373. Springer (2013)
5. Verdon, D., McGraw, G.: Risk analysis in software design. Security Privacy, IEEE 2(4), 79–84 (July 2004)