
Empirical Study of the Security Requirements Engineering Process in Practical Context

Date: 23-08-2013

Kate Labunets, Tong Li, Vlad Acretoaie
ERMI Summer School 2013

Research Goal

We study <property: the performance> of <objects: security analysts> in <setting: security requirements analysis> under <treatment: the application of SREP> in order to <purpose: assess the applicability of the SREP in industrial settings> by <method: conducting a field study with an industrial company>.

Research Methodology:

Systematic Literature Review



Systematic Literature Review

- **RQ1**: Which metrics are used for evaluating security requirements methodologies?
- **RQ2**: How do existing methodologies perform according to the identified metrics?
- Preliminary search term:
`security AND requirements AND
(metrics OR performance) AND
(evaluation OR study)`

Systematic Literature Review

→ Inclusion criteria:

- ◆ Studies presenting security requirements methodology evaluation metrics
- ◆ Studies applying security requirements methodology evaluation metrics
- ◆ Studies written in English

→ Exclusion criteria:

- ◆ Studies lacking any kind of validation (i.e. opinion pieces)

Systematic Literature Review

→ Data to extract for each metric:

- ◆ Maturity (based on introduction date and known application instances)
- ◆ Application conditions
- ◆ Application methodology
- ◆ Nature and reliability of existing application results

→ Data analysis goal:

- ◆ Ranking evaluation metrics based on their maturity, reliability, and applicability

Research Methodology:

Focus Group Interview



Focus Group Interview

- **Goal:** Investigate practical performance and metrics of security analysis in company XXX.
- **Subjects:** 2-5 security (requirements) analysts in company XXX.
- **Environment settings:** A small size meeting room (less than 10 people). A video recorder is set in the corner of the room to record the whole procedure of the interview.

Focus Group Interview

Pre-defined questions:

1. How do you analyze security requirements?
2. Have you ever been using certain security requirement methods?
3. How many efforts do you spend on security requirement analysis?
4. How do you evaluate quality of elicited security requirements?
5. Do you refer to any security standards? If so, which ones?
6. What are the advantages of your current practices?
7. What are the disadvantages of current practices?

Research Methodology:

Case Study



Case Study: Goal & Context

→ What the purpose is?

Assess the applicability of the SREP in industrial context

→ What the context is?

- ◆ international company providing full cycle of software development (SD) services,
- ◆ real SD project,
- ◆ project team of 3-5 professionals (SA, BA, Security Analyst, Software Architect),
- ◆ full access to project team and data.

Case Study: Data & Validation

→ How to collect data?

Interview, observation of project meetings (work sessions), project diaries, project reports, project postmortem analysis.

→ How to analyse data?

Grounded theory (coding) and researcher's brain.

→ How to validate findings?

- ◆ ask subjects what they think about our findings,
- ◆ map findings with existing studies (if they are), or
- ◆ run further empirical studies.

Summary

Research Goal:
Assess SREP in industrial context

**Systematic
Literature
Review**

**Focus
Group
Interview**

**Case
Study**

Outcomes:
Assessment of the SREP applicability in industrial context