ICSE 2024

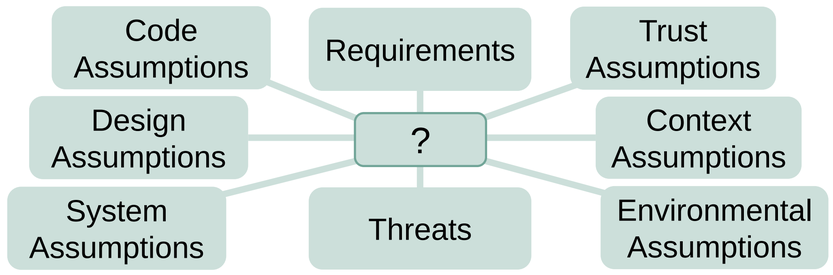
# What do you assume?
# A Theory of Security-Related Assumptions

Sophie Corallo, Thomas Weber, Lars König, Kathrin Leonie Schmidt, Frederik Reiche, Anne Koziolek

## Motivation

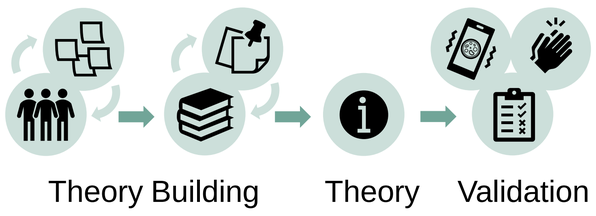
**Implicit**, **inconsistent**, or **invalid** assumptions about the system can have a **high impact** on the **system**, e.g., on its security

**No shared notion** of *Assumption*



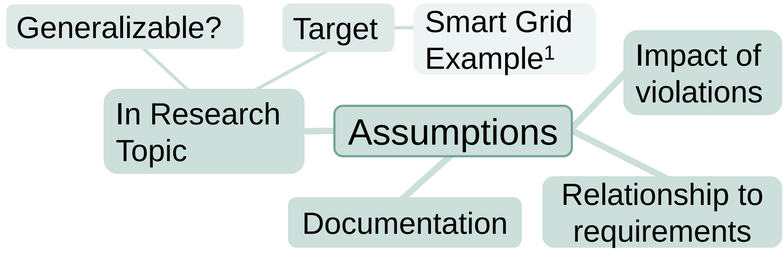

**RQ1a**: **What** is an assumption?
**RQ1b**: What are its **relations to software artifacts**?
**RQ2**: Is there a **difference** between the notions?
**RQ3**: What should be **documented**?

### Research Process

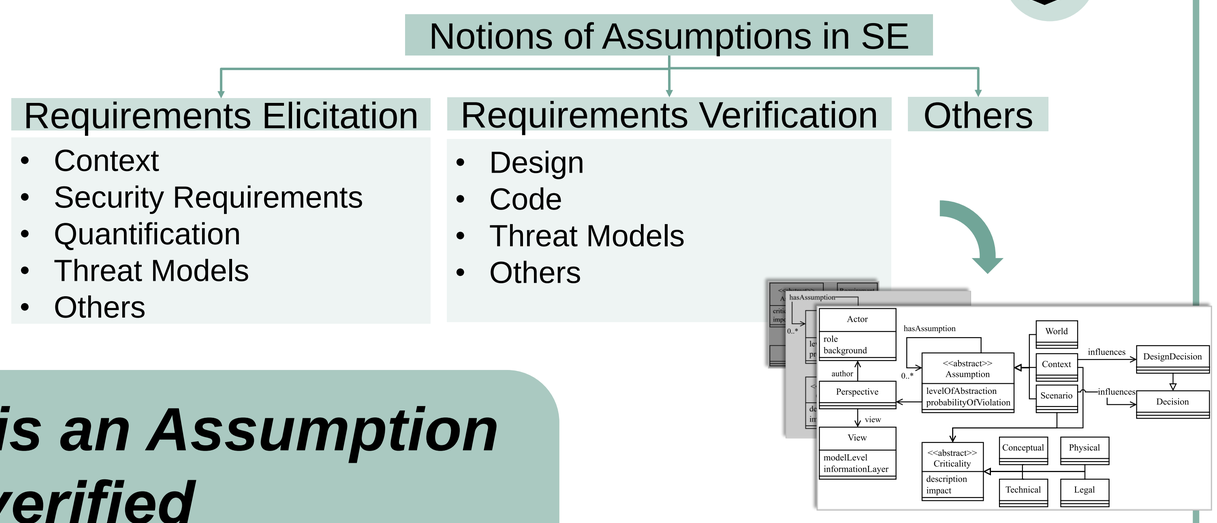



## Theory Building

**Interviews** with 9 security researchers



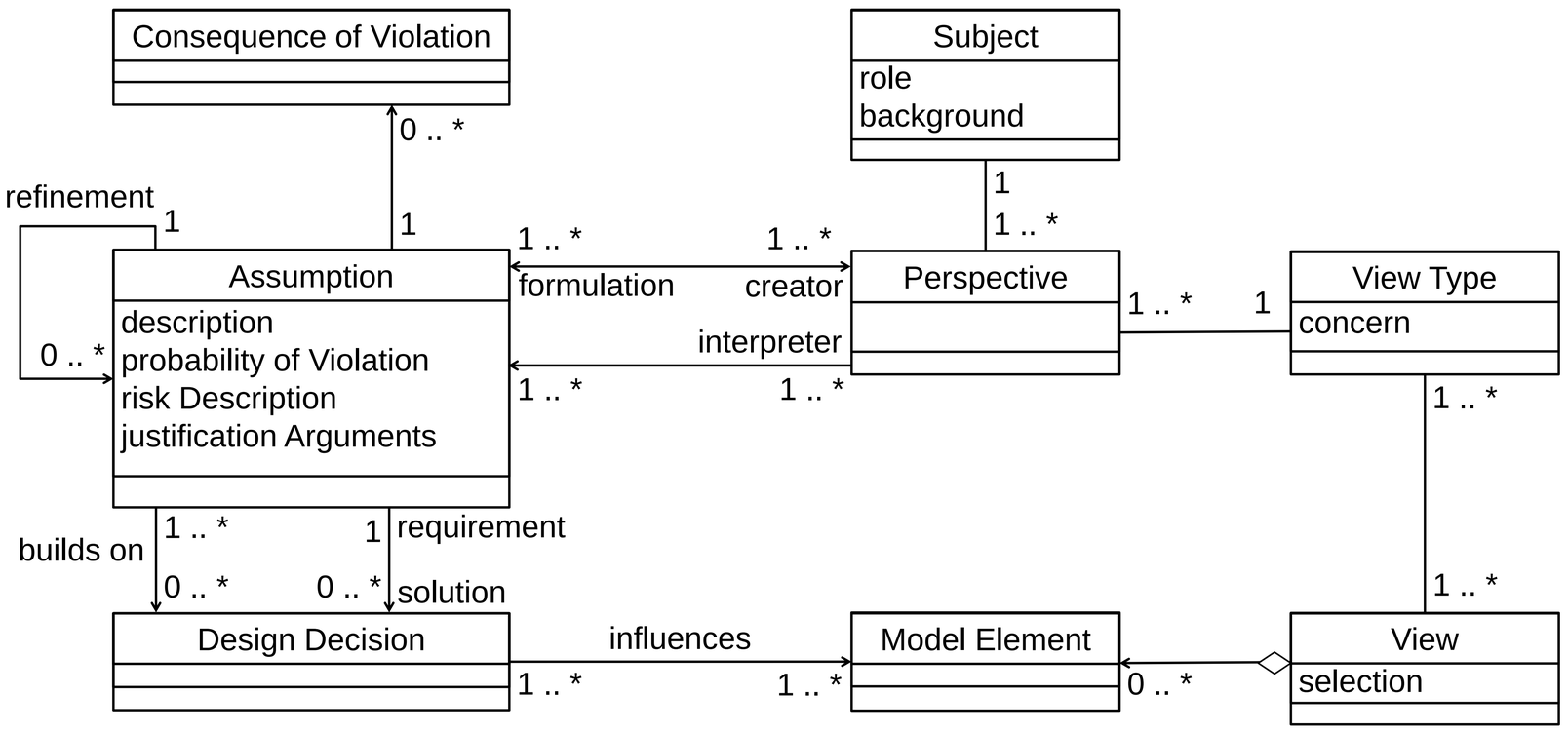

**Literature Review** of 53 scientific publications




***Every Requirement is an Assumption until it's verified***

*However, what is an assumption?*

## Theory & Definition




Assumptions …

- are **taken for true** and can be **violated**,
- are **formulated from a certain perspective** and can be **interpreted differently** from different perspectives,
- can be **refined** horizontally & vertically,
- **occur when a design decision** is made,
- **transform into a requirement** if they are supposed to be realized by a design decision,
- have a **probability of being violated**,
- have **consequences** of their violation,
- are a **risk** to the system

## Validation

### Example based on Case Study CWA[2]

Assumptions are derived based on the documented risks of the CWA. These assumptions are represented according to the proposed scheme.

| No & Description | Risk | Consequence | View Type | Design Decision |
|---|---|---|---|---|
| [48] The network connection between the device of the user and the servers is secure | Disclosure of personal data in network traffic | Data leakage | Communication | Trust assumption |

### Questionnaires

- 81 Software engineers: Security-Related Assumptions
- 67 Software engineers: Assumptions in Software Engineering

☑ **Agreement to every property**

☑ **Applies to all assumptions in software development**

## Conclusion

→ **Possible transfer of approaches** from requirements to assumptions, e.g., for assumption elicitation, maintenance, verification

→ Assumptions **should be traced** to software artifacts

→ Assumptions are **perspective dependent**

→Assumptions in software development **base on the same definition**

### Sources

[1] P. Van Aubel and E. Poll. 2019. Smart metering in the Netherlands: What, how, and why. International Journal of Electrical Power & Energy Systems 109 (2019)

[2] Robert Koch Institute. 2020. Open-Source Project Corona-Warn-App. https: //www.coronawarn.app/en/.

Publications, Supplementary Material & more: https://secdragon-dev.github.io/WhatDoYouAssume/