**Interview Guide (translated for publication)**

**Statistical Data**

Job title ________________________________________

Years of experience ________________________________________

Size of enterprise ________________________________________

Domain ________________________________________

Procedure Model ________________________________________

Importance of Security in the
participant's current projects ________________________________________

*do some general explanations*

**Architectural Security Rules in general**

1. What **threats** do you see for **software** systems in your software projects?
   - *How do you assess the need for software-level security measures compared to measures at the hardware and infrastructure level?*
   - *Which security measures should be taken in software systems?*
2. At what point in the **development process**, security is considered in your experience?
3. How do you assess the impact of the **software architecture** on a software product's security level?
4. What **measures** are taken during **architecture design** in your experience?
5. How do you enforce that the architecture is implemented as planned?

**Architectural Security Rules**

6. What **architectural rules for security** are specified in software architectures, **today**?

*Show exemplary architectural security rules*

7. How relevant do you assess architectural security rules in your projects?
   - How relevant do you assess architectural security rule violations as the third category of software vulnerabilities in addition to security design flaws and code-level security bugs?
8. How would you enforce the implementation's conformance with the exemplary architectural security rules?
9. What relevance should architectural security rules have in software development?
10. Which conditions must be met for architectural security rules to be taken into account in industry?
11. What impediments hinder industry from explicitly specifying architectural security rules?

**Identification Process**

*Explain identification process and show supporting questions*

12. How do you assess the described identification process with regard to their suitability to identify relevant architectural security rules?
13. Which questions would you add or omit?
14. What other sources of architectural security rules do you consider relevant or necessary?
15. How do you assess the procedure’s applicability in order to identify additional, project-specific architectural security rules?
16. How do you assess the need to supplement the rule set with project-specific architectural security rules?
    a. Can you think of any examples of project-specific architectural security rules?

### Catalogue of Architectural Security Rules

17. How could a catalogue of architectural security rules support the development of secure software systems?
    a. How do you assess the benefits of such a catalogue in general?
    b. How do you assess the cost/benefit ratio of such a catalogue?
    c. What impediments can you think of for implementing and maintaining such a catalogue?

*Show (paper) prototype of the catalogue*

18. How do you assess the value of the prototyped catalogue?
    a. What information would you add to improve its usefulness?
    b. What functionality would you add to enhance its usefulness?
    c. Do you have any further suggestions for improving the catalogue?
    d. How would you use such a catalogue?
    e. In what situation would you use the catalogue?
19. How much effort in using the catalogue would be acceptable for a software architect for using the catalogue?
20. What impediments to use the catalogue can you think of?

### Security Conformance Checking

21. Let's assume that there is a conformance checking tool that is connected to this catalogue and is able to use the specified architectural security rules from this catalogue:
    a. How interesting would such a tool be for you?
    b. What initial effort would be acceptable for a software architect for using such a conformance checking tool (setup, selecting the relevant rules, specify the architecture-to-code-mapping etc.)?
    c. What continuous effort would be acceptable for a software architect for using such a conformance checking tool (execute conformance check, monitor and prioritize results etc.)?
    d. What initial effort would be acceptable for a software developer for using such a conformance checking tool (installing plugins etc.)?
    e. What continuous effort would be acceptable for a software developer for using such a conformance checking tool (execute conformance check, check results etc.)?
22. If you could wish something:
    a. How would you like to specify the intended/planned architecture?
    b. How would you like to select or specify the architectural security rules?

c. How would you like to map security-related architectural concepts to source artefacts?

23. How should the violations be reported?
    a. How detailed should the violation report be?
    *Examples, if needed: code lines, input values that triggered violating behaviour etc.*
    b. How should the violations be presented?