Analyzing UML Models for Security Requirements using CARiSMA

Nupur Chandrashekhar Deshmukh (223201702)

University of Koblenz

1 Introduction

- Security issues often arise due to a combination of preconditions and triggers.
- Difficulty in reconstructing and diagnosing root causes of security breaches or privacy problems.
- The importance of maintaining a record of relevant events and decisions.
- Utilizing UML model-level security analysis to enhance system security explainability.

2 Analytical Framework and Methodology

2.1 Research Questions

- RQ 1: Specifying security properties within a UML context.
- RQ 2: Analyzing security properties automatically using CARiSMA.
- RQ 3: Application of CARiSMA to data spaces scenario

2.2 CARisMA Overview

- CARiSMA: Compliance, Risk, and Security Model Analyzer.
- Capabilities: compliance, risk, and security analyses of software models.
- Evolution from UMLsec tool to support UML models natively.
- Integration with Eclipse and various modelling tools like Papyrus MDT, and IBM Rational Software Architect.
- Flexible plugin architecture for extending CARiSMA for new languages and custom checks.

2.3 Methodology

- Utilization of CARiSMA tool for analysing UML models for security requirements.
- Practical component involving reporting on the task and demonstration in the presentation.
- Guidance and supervision by Prof. Dr. Jan Jürjens.

2.4 Specifying Security Properties in UML Context

- Examination of methods for representing security properties within UML diagrams.
- Identification of relevant elements such as classes, objects, interactions, and constraints.
- Consideration of security requirements like authentication, authorization, confidentiality, and integrity.

2.5 Analyzing Security Properties with CARisMA

- Workflow for integrating UML models into CARiSMA.
- Utilization of compliance, risk, and security analysis features
- Automatic identification of security vulnerabilities and risks.
- Interpretation of analysis results and their implications for system security.

3 Data Space Overview

- Introduce the concept of data spaces and their significance in modern computing environments.
- Discuss the characteristics and challenges associated with data spaces.
- Provide examples of data space applications and their relevance to security analysis.

4 Security Requirements in Data Spaces

- Explore the specific security requirements and challenges inherent to data spaces.
- Discuss issues such as data access control, privacy, data integrity, and data sharing within data spaces.
- Analyze the implications of security breaches in data space environments.

5 CARiSMA Application in Data Spaces

- Describe how CARiSMA can be adapted and applied to analyze security properties within data space environments.
- Present methodologies for integrating data space models into CARiSMA for analysis.
- Discuss the benefits and limitations of using CARiSMA in data space security analysis.

6 Effectiveness Demonstration

- Provide a practical demonstration showcasing how CARiSMA effectively addresses security issues in data space scenarios.
- Present case studies or examples illustrating CARiSMA's ability to identify and mitigate security vulnerabilities within data spaces.
- Discuss the outcomes and implications of the effectiveness demonstration.

7 Conclusion

- Summary of findings regarding the specification and analysis of security properties in UML models using CARiSMA.
- Implications for enhancing security explainability and mitigating risks in software systems.
- Future research directions and potential improvements in utilizing CARiSMA for security analysis.

8 References

- List of sources and literature consulted during the research process.