KASTEL – Institute of Information Security and Dependability
Modelling for Continuous Software Engineering (MCSE)
Dependability of Software-intensive Systems (DSiS)
Prof. Koziolek & Prof. Reussner

Modellierung und Analyse von Sicherheitsannahmen

Beschreibung

Einer der ersten Schritte der Softwareentwicklung ist die Anforderungserhebung. Beispielsweise soll das System sicher gegen einen bestimmten Angriff sein. Implizit sind in solchen Anforderungen Annahmen enthalten von denen die Erfüllung der Anforderung abhängt. Bleiben solche Annahmen undokumentiert entstehen Unsicherheiten und Fehler.

Durch eine Analyse getätigter sicherheitsbezogener Annahmen auf verschiedenen Sichten (z.B. Architektur, Code) könnten Misskonzeptionen und hieraus entstehende Sicherheitslücken erkannt werden. Zu diesem Zwecke müssen passende Sicherheitsanalysen ausgewählt und klassifiziert werden. Anschließend können Annahmen den Analysen zugeordnet und evaluiert werden.

Beispiel *Das System hat die Anforderung, dass personenbezogene Daten DSGVO-konform behandelt werden. Dies inkludiert u.a., dass alle Datenbanken mit pers. Daten sich in vertrauenswürdigen Ländern befinden und verschlüsselt werden. Zur Überprüfung stehen Ihnen nun mehrere Sicherheitsanalysen zur Verfügung. Eine kann Deployment-Informationen überprüfen, während andere den Informationsfluss oder die Verschlüsselung zwischen Architekturelementen überprüft. Das Ziel ist nun die Annahmen so zuzuordnen, dass sie durch die jeweiligen Analysen evaluiert werden können. Das Ergebnis könnte dann eine Art Annahmenbaum sein, in dem sichergestellte und abgelehnte Annahmen markiert werden. Somit könnte man bereits anhand der Architektur automatisch feststellen ob Anforderungen korrekt geplant wurden oder nicht.*

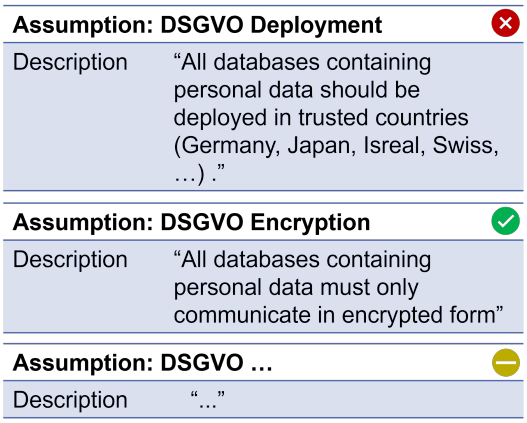

Abbildung: Evaluierte Annahmen des Beispiels

Sonstiges

Das Thema schließt direkt an unsere aktuelle Forschung an und bietet Publikationsmöglichkeiten. Eine Veränderung des Themas auf Wunsch der Teilnehmer ist möglich.

Wir empfehlen das Thema für 2 Studierende. Für mehr oder weniger Studierende kann der Umfang angepasst werden.

Kontakt

Sophie Corallo (sophie.schulz@kit.edu), Frederik Reiche (frederik.reiche@kit.edu)