

Architekturbasierte Modellierung von Sicherheitsmuster für Enterprise-Anwendungen

Moderne und komplexe Enterprise-Software-Systeme durchlaufen im Laufe der Zeit viele Änderungen mit unterschiedlichen Folgen für die Sicherheit des Systems. Um diese Folgen schnell und präzise erkennen sowie darauf reagieren zu können, sollte Sicherheit bereits in früheren Entwicklungsphasen und danach kontinuierlich betrachtet werden. Dazu müssen auf Architekturebene Modellierungsmöglichkeiten geschaffen werden, um die sicherheitsrelevante Entwurfsentscheidungen mit dazugehörigen Annahmen an den Systemkontext, die Laufzeitkonfiguration sowie Nutzungsprofile zu dokumentieren. Die als eine logische Verbindung zwischen Bedrohungen und Sicherheitsmuster agierende Annahmen werden eingesetzt, um die Validität der Sicherheitsaspekte zu überprüfen. Die so entstandenen Sichten und Modelle können anschließend in den verschiedenen Phasen zur Analyse der Sicherheit genutzt werden, u.a. auf sicherheitsrelevante Änderungen während der Software-Evolution. Im Rahmen der Forschungsgruppe soll ermittelt werden, wie formale Dokumentation von Annahmen und deren Analyse bzgl. Sicherheitsaspekte genutzt werden können, um Sicherheitszustand einer Enterprise-Anwendung während der Software-Evolution zu prüfen. Dabei sollen insbesondere folgende Punkte betrachtet werden:

- Untersuchung unterschiedlicher Sicherheitsaspekte für konkrete Anwendungsdomäne- und Szenarien (Webanwendungen, Betriebssysteme, eingebettete Software, etc.)
- Ableitung der möglichen Sicherheitslücken, Bedrohungen sowie dazugehörige Annahmen aus Antipatterns und Misuse-Cases
- Abbildung von Laufzeitkonfiguration und deren Beschreibung während der Entwurfsphase

Der entwickelte Ansatz soll zur Evaluation in der PCM-Workbench umgesetzt werden. Als Fallstudienystem wird CoCoMe genutzt. Es handelt sich dabei um eine Cloud-basierte, verteilte Enterprise-Anwendung, für die verschiedene State-of-The-Art Evolutionsszenarien definiert wurden.

Ansprechpartner:

- Emre Taşpolatoğlu (taspolat@fzi.de)
- Robert Heinrich (heinrich@kit.de)