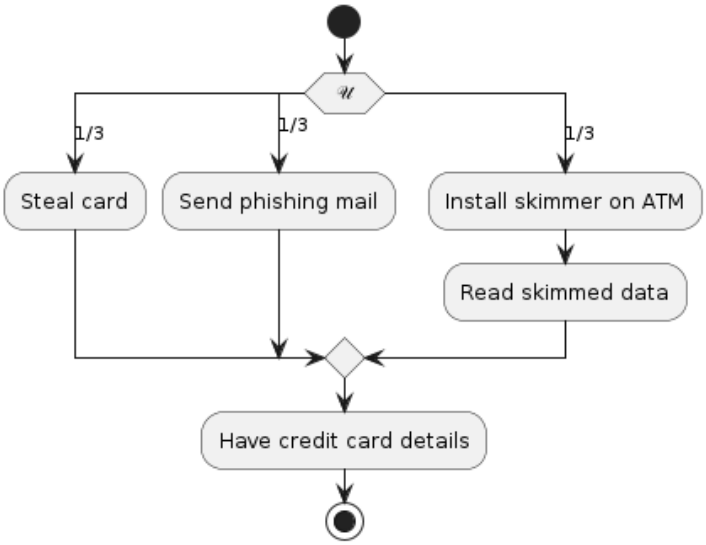
Karlsruher Institut für Technologie

Institut für Informationssicherheit und Verlässlichkeit (KASTEL)
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

Masterarbeit oder Praxis der Forschung

Modellierung von Angriffen für quantitative Sicherheitsanalysen



Hintergrund. Die meisten Methoden für formale Softwareverifikation geben ein binäres Ergebnis aus: Die Software ist entweder korrekt oder nicht. Qualitätsmaße wie Testabdeckung sind selten robust. In einer Zusammenarbeit der Lehrstühle Prof. Beckert und Prof. Reussner entstand deshalb ein Ansatz zur formalen quantitativen Verifikation der Software-Zuverlässigkeit. Zuerst ermittelt das Verifikationswerkzeug KeY alle Eingaben, für die die Korrektheit der Software nicht bewiesen werden kann. Diese kritischen Eingaben werden dann zum einem in dem Modellierungswerkzeug Palladio erstellten Architekturmodell hinzugefügt. Palladio fügt die kritischen Eingaben, ein Nutzermodell und eine Verhaltensbeschreibung der Software zu einem probabilistischen Programm zusammen und ermittelt so die Fehlerwahrscheinlichkeit. Allerdings ist dieser Ansatz bisher auf funktionale Korrektheit beschränkt. Eine Analyse, die auch einen Angreifer berücksichtigt, ist bisher nicht möglich.

Aufgabe. Ihre Aufgabe ist es, eine Angreifermodellierung als Erweiterung des Palladio-Komponentenmodells zu entwickeln. Die Modellierung sollte es erlauben, Szenarien als Angriffsbäume (Flowcharts wie im Beispiel oben) zu beschreiben, wobei das Verhalten des Angreifers sowohl probabilistisch (der Angreifer wählt eine zufällige Handlungsoption) als auch possibilistisch (der Angreifer weiß, welche Handlungsoption die beste Erfolgswahrscheinlichkeit birgt, und verhält sich entsprechend) auftreten kann. Die Quantifizierung der Sicherheit bezieht sich dann auf die Kosten und Schwere möglicher Angriffe.

Kontakt
Florian Lanzinger lanzinger@kit.edu Büro 50.34R227