

## Bachelorarbeit

# Quantifizierte Sicherheitsausagen mit Probabilistischen Model-Checker

### Ist dieses Programm korrekt?

```
/*@ requires amount >= 0 && cc.length() == 12;  
   @ ensures \exists int i; mQueue[i].cc = cc  
           && mQueue[i].amount = amount;  
   @*/  
public void createInvoice(String cc, int amount) {  
    if(amount < 0) throw new IllegalArgumentException();  
    if(cc.length != 12) throw new IllegalArgumentException();  
  
    //exclude company credit card for testing purpose  
    if( cc.startsWith("4570") && cc.endsWith("6172")) {  
        return;  
    }  
  
    billingService.send(new Invoice(cc, amount));  
}
```

Anscheinend nicht; der Entwickler hat für Testzwecke seine Kreditkarte von der Rechnungserstellung ausgeschlossen und war dabei unpräzise. Eine Backdoor wie ein Weihnachtsgeschenk für all diejenigen mit der richtigen Kartenummer.

*Aber wie hoch wäre das Eintrittswahrscheinlichkeit  
dieses Fehlers im operativen Betrieb?*

In dieser Bachelorarbeit möchten wir eben diese Frage für *unsichere* Software beantworten unter der Verwendung von probabilistischen Model-Checkers.

### **Aufgabe.**

Diese Arbeit umfasst die Einarbeitung in das Forschungsfeld der probabilistischen Model-Checkers, das Modellieren Java-Programmen in probabilistische Modelle, sowie die Evaluation der Machbarkeit und Grenzen zur Quantifizierung von Abweichungen zur Spezifikation.

**Ihr Profil.** Solide Kenntnisse im Bereich der Java-Programmierung und Stochastik erforderlich. Ebenso sollte Formale Systeme am KIT (oder vergleichbarer Kurs) erfolgreich abgeschlossen.

### **Kontakt**

Jonas Schiffl/Alexander Weigl    {jonas.schiffl,weigl}@kit.edu    Office: 50.34, R22{5,6}