

## Übungen zur Vorlesung „Betriebssysteme“

### Blatt 10

#### Aufgabe 39

James Bond, der Geheimagent 007 ihrer Majestät, wird häufig in gefährliche Missionen geschickt, bei denen er sich mit anderen Geheimagenten treffen muß. Die meisten der Agenten kennen sich untereinander nicht, um das Enttarnen durch gegnerische Geheimdienste zu erschweren; schließlich kann es immer mal wieder einen Verräter geben. Der Einzige, der alle Agenten kennt und mit ihnen in Kontakt treten kann ist der Geheimdienstchef M. Bei seiner aktuellen Mission erfährt 007, daß der junge „Vorstadtagent“ Jimmy Bondi wichtige Geheiminformationen zusammengetragen hat. Bedauerlicherweise kennt James jedoch weder Aufenthaltsort noch Aussehen von Jimmy. Beschreiben Sie, wie James nach dem Muster des Needham-Schroeder-Authentisierungsprotokolls mit Jimmy Kontakt aufnehmen kann.

#### Aufgabe 40

Seit einiger Zeit kommt es manchmal zu einer Zusammenarbeit des englischen Secret Service mit dem KGB. Das Vertrauen zueinander wächst zwar, die Identitäten und Aufenthaltsorte der Agenten bleiben jedoch weiterhin streng geheim. So kennt nach wie vor nur M alle englischen Agenten und nur der russische Geheimdienstchef kennt alle russischen Agenten. James Bond hat erfahren, daß im Rahmen einer Zusammenarbeit mit dem KGB eine russische Agentin mit ihm zusammentreffen soll. Um bei seinen vielen weiblichen Bekanntschaften sicher zu sein, daß er mit der richtigen Person zusammenarbeitet, muß (zumindest der erste) Kontakt auf einem sicheren Weg hergestellt werden. Erweitern Sie zu diesem Zweck das Needham-Schroeder-Protokoll bzw. entwerfen Sie ein geeignetes eigenes Authentisierungsprotokoll.

#### Aufgabe 41

- Geben Sie für alle vorgestellten Deduktionsregeln der BAN-Logik an, welche Annahmen bzw. Voraussetzungen zusätzlich notwendig sind und in dem Buch von Coullouris, Dollimore und Kindberg ([CDK]) fehlen.
- Beweisen oder widerlegen Sie mit Hilfe der „reparierten“ Deduktionsregeln

$$\frac{\text{fresh}(X), P \text{ said } (X, Y)}{P \text{ believes fresh}(X, Y)}, \quad \frac{P \text{ believes } (Q \text{ said } X), Q \text{ sees fresh}(X, Y)}{P \text{ believes } Y}.$$

- Geben Sie für den „Beweis“ zur Sicherheit des Needham-Schroeder-Protokolls in [CDK] alle Lücken und alle hierbei zusätzlich notwendigen Annahmen an.
- Geben Sie an, wo im Zusammenhang mit der BAN-Logik inkonsistente bzw. sogar „verbotene“ (undefinierte) Schreibweisen benutzt werden, und versuchen Sie diese Inkonsistenzen zu beseitigen.

#### Aufgabe 42\*

Entwerfen Sie ein formales Logiksystem, mit dem Sie die Korrektheit von Authentisierungsprotokollen (oder anderen Protokollen) nachweisen können.