19. April 2012

# Protokollsicherheit

## Blatt 1

**Aufgabe 1-1.** Im dritten Versuch zum Entwurf des Protokolls aus der ersten Vorlesung hätte man auch folgende Möglichkeit vorschlagen können:

$$\begin{aligned} &1.\ A \to S: && \langle A, B\rangle \\ &2.\ S \to A: && \{\langle K_{AB}, B\rangle\}_{K_{AS}} \\ &3.\ S \to B: && \{\langle K_{AB}, A\rangle\}_{K_{BS}} \end{aligned}$$

Zeigen Sie, dass dieses Protokoll den Schlüsselaustausch zwischen $A$ und $B$ nicht garantiert.

**Aufgabe 1-2.** In folgendem Protokoll zum Austausch eines von $A$ erzeugten Schlüssels $K$ zwischen $A$ und $B$ wollten die Entwickler besonders vorsichtig sein und haben deshalb beschlossen, den Schlüssen innerhalb der Nachricht ein zweites Mal zu verschlüsseln.

$$\begin{aligned} A \to B: &\quad \{\langle A, \{K\}_{\mathsf{pk}(B)}\rangle\}_{\mathsf{pk}(B)} \\ B \to A: &\quad \{\langle B, \{K\}_{\mathsf{pk}(A)}\rangle\}_{\mathsf{pk}(A)} \end{aligned}$$

Zeigen Sie, dass ein Angreifer den Schlüssel $K$ erfahren kann, auch wenn sich $A$ und $B$ weiterhin ehrlich verhalten.

Welche weiteren Probleme sehen Sie, auch wenn die zusätzliche Verschlüsselung von $K$ weggelassen wird?

**Aufgabe 1-3.** Im Otway-Rees Protokoll ist es wichtig, dass $S$ in Nachricht 2 überprüft, dass die drei Vorkommen von $M$ übereinstimmen.

$$\begin{aligned} &1.\ A \to B: M, A, B, \{N_A, M, A, B\}_{K_{AS}} \\ &2.\ B \to S: M, A, B, \{N_A, M, A, B\}_{K_{AS}}, \{N_B, M, A, B\}_{K_{BS}} \\ &3.\ S \to B: M, \{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}} \\ &4.\ B \to A: M, \{N_A, K_{AB}\}_{K_{AS}} \end{aligned}$$

Prüft $S$ nur dass die letzteren beiden Vorkommen von $M, A, B$ übereinstimmen, so kann ein Angreifer $C$ erreichen, dass er anstelle von $B$ den Schlüssel $K_{AB}$ mit $A$ teilt. Können Sie einen solchen Angriff finden?

**Aufgabe 1-4.** In welchem der folgenden Fälle ist es möglich, einen CCS-Prozess $P$ zu finden, so dass der jeweilige Prozess irgendwann einmal dazu kommt eine $\overline{c}$-Aktion auszuführen? Wie muss $P$ jeweils lauten?

a) $b.(\overline{a}.0 \mid a.\overline{c}.0) \mid P$

b) $b.(\overline{a}.0 + a.\overline{c}.0) \mid P$

c) $b.(c.0 \mid \overline{c}.a.0) \mid P$

d) $b.(\nu a.\,(\overline{a}.0 \mid a.\overline{c}.0)) \mid P$

e) $\nu a.\,(\overline{b}.0 \mid a.\overline{c}.0) \mid P$