Universität Duisburg-Essen **SS 2019**
Ingenieurwissenschaften / Informatik **2. Juli 2019**
Dozent: Prof. Dr. Barbara König **Übungsblatt 6**
Übungsleitung: Richard Eggert **Abgabe: -**

Formale Aspekte der Softwaresicherheit und Kryptographie

Hinweis: Dies ist kein Testatblatt; reichen Sie bitte keine Lösungen ein!
Dieses Übungsblatt wird am 11.07 besprochen.

Aufgabe 22 Inkorrektes Protokoll

Folgendes Protokoll mit symmetrischer Verschlüsselung ist ganz offensichtlich falsch, wenn die Nachricht m geheimgehalten werden soll:

- $A \to B$: K
- $B \to A$: $\{m\}_K$

(a) Modellieren Sie das Protokoll im angewandten π-Kalkül, wobei Sie annehmen, dass zu Beginn des Protokolls nur A den Schlüssel K und nur B die Nachricht m kennt.

(b) Übersetzen Sie die Prozesse in Hornklauseln. Stellen Sie auch eine entsprechende Zielklausel auf und statten Sie den Angreifer mit geeignetem Vorwissen aus.

(c) Zeigen Sie, dass aus der Klauselmenge die leere Klausel ableitbar ist.

Aufgabe 23 Nonce-Challenge in ProVerif

Installieren Sie das ProVerif-Tool (erhältlich unter `http://proverif.inria.fr/`). Modellieren Sie dann das Nonce-Challenge-Protokoll von den Vorlesungsfolien und überprüfen Sie, dass der Nonce geheimgehalten wird.

Aufgabe 24 Wide-Mouthed-Frog-Protokoll

Betrachten Sie das folgende Protokoll (sogenanntes Wide-Mouthed-Frog-Protokoll), an dem Alice (A), Bob (B) und der Server (S) beteiligt sind. Dabei teilen sich sowohl Alice als auch Bob einen Schlüssel mit dem Server (K_{AS} bzw. K_{BS}).

- $A \to S$: $\{K_{AB}\}_{K_{AS}}$ (auf dem Kanal c_{AS})
- $S \to B$: $\{K_{AB}\}_{K_{BS}}$ (auf dem Kanal c_{BS})
- $A \to B$: $\{M\}_{K_{AB}}$ (auf dem Kanal c_{AB})

D.h., Alice denkt sich einen Sitzungsschlüssel aus, den sie über den Server zu Bob schickt. Durch das Senden der letzten Nachricht authentifiziert sie sich gegenüber Bob.

(a) Modellieren Sie dieses Protokoll in ProVerif. Sie können dabei annehmen, dass der Server ausschließlich dazu da ist, Nachrichten von Alice anzunehmen und an Bob weiterzuleiten.

(b) Überlegen Sie sich, wie man die Authentifizierung spezifizieren kann.

(c) Verifizieren Sie das Protokoll mit Hilfe von ProVerif.