Aufgabe 6: BAN-Logik und Needham/Schroeder-Protokoll für geheime Schlüssel

Systemsicherheit

Übungsblatt 6
Stephan Beyer
Team 2

Systemsicherheit SS'08
Technische Universität Ilmenau

30. Juni 2008

Übungsblatt 6, Aufgabe 2

Beweisen Sie mittels *BAN-Logik*, dass für das *Needham/Schroeder*-Authentisierungsprotokoll für *geheime Schlüssel* gilt:

$$B \models A \leftrightarrow^{K_{AB}} B$$

d. h. nach einem Protokollablauf glaubt B, dass der geheime Sitzungsschlüssel, den B sich mit A teilt, K_{AB} ist.

Grundlagen: BAN-Logik

Notationen

Principals A, B, Formel X, Schlüssel K_{AB}:

$A \models X$	A glaubt, dass X wahr
$A \lhd X$	A sieht X, d. h. kann X in eigene Nachrichten einbauen
$A \mid\sim X$	A sagt X, d. h. $A \models X$ und verschickt Botschaft mit X
$A \Rightarrow X$	A hat Autorität bzgl. X
$\mathrm{fresh}(X)$	X ist frisch, d. h. wurde nie zuvor verschickt
$A \leftrightarrow^{K_{AB}} B$	A und B können K_{AB} benutzen

Grundlagen: BAN-Logik (2)

Deduktionen

- Botschaften-Semantikregel

$$\frac{A \models A \leftrightarrow^{K_{AB}} B, \quad A \lhd \{X\}_{K_{AB}}}{A \models B \mid\sim X}$$

- Nonce-Validierungsregel

$$\frac{A \models \mathrm{fresh}\,(X)\,, \quad A \models B \mid\sim X}{A \models B \models X}$$

- Autoritätsregel

$$\frac{A \models B \mid\Rightarrow X, \quad A \models B \models X}{A \models X}$$

- (De-)Kompositionsregeln ...

Grundlagen: Needham/Schroeder-Protokoll

Ziel:

- A will symmetrisch verschlüsselte Verbindung mit B aufbauen
- Sicherstellung: A ist wirklich A, B ist wirklich B
- (frischer) Schlüssel K_{AB} soll von Authentisierungsserver geholt werden

Ablauf

1. $A \rightarrow S : A, B, N_A$
2. $S \rightarrow A : \{N_A, B, K_{AB}, \{A, K_{AB}\}_{K_{BS}}\}_{K_{AS}}$
3. $A \rightarrow B : \{A, K_{AB}\}_{K_{BS}}$ (daraus folgt idealisiert: $B \lhd \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}$)
4. $B \rightarrow A : \{N_B\}_{K_{AB}}$
5. $A \rightarrow B : \{N_B - 1\}_{K_{AB}}$ (daraus folgt idealisiert: $B \lhd \text{fresh}\left(\{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}\right)$)

Grundannahmen

Für das Funktionieren des Protokolls wird u. A. angenommen:

- bekannte Schlüssel:

$$B \models B \leftrightarrow^{K_{BS}} S$$

- Vertrauen in den Server:

$$B \models S \Rightarrow A \leftrightarrow^{K_{AB}} B$$
$$B \models S \Rightarrow \text{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)$$

- Vertrauen in sich selbst:

$$B \models \text{fresh}\left(N_B\right)$$

Schlechte Nachricht

Es ist uns nicht gelungen, für das angegebene Protokoll zu beweisen, dass

$$B \models A \leftrightarrow^{K_{AB}} B$$

Beweisen, was geht...

$$\frac{B \models B \leftrightarrow^{K_{AB}} S, \quad B \lhd \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}}{A \models S \mid\sim A \leftrightarrow^{K_{AB}} B}$$

:(

Herangehensweise: „von unten“

$$\frac{}{B \models A \leftrightarrow^{K_{AB}} B}$$

Herangehensweise: „von unten“

$$\frac{B \models S \Rrightarrow A \leftrightarrow^{K_{AB}} B, \qquad \dfrac{}{B \models S \models A \leftrightarrow^{K_{AB}} B}}{B \models A \leftrightarrow^{K_{AB}} B}$$

Herangehensweise: „von unten“

$$\frac{B \models S \Rrightarrow A \leftrightarrow^{K_{AB}} B, \quad \dfrac{\dfrac{}{B \models \mathrm{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}, \quad \dfrac{}{B \models S \mid\!\sim A \leftrightarrow^{K_{AB}} B}}{B \models S \models A \leftrightarrow^{K_{AB}} B}}{B \models A \leftrightarrow^{K_{AB}} B}$$

Herangehensweise: „von unten“

$$\frac{B \models S \Rrightarrow A \leftrightarrow^{K_{AB}} B, \quad \frac{\frac{\dots}{B \models \mathrm{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}, \quad \frac{\dots}{B \models S \mid\!\sim A \leftrightarrow^{K_{AB}} B}}{B \models S \models A \leftrightarrow^{K_{AB}} B}}{B \models A \leftrightarrow^{K_{AB}} B}$$

$$\frac{}{B \models S \mid\!\sim A \leftrightarrow^{K_{AB}} B}$$

$$\frac{}{B \models \mathrm{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}$$

Herangehensweise: „von unten“

$$\frac{B \models S \Rrightarrow A \leftrightarrow^{K_{AB}} B, \quad \frac{\frac{\dots}{B \models \text{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}, \quad \frac{\dots}{B \models S \mid\sim A \leftrightarrow^{K_{AB}} B}}{B \models S \models A \leftrightarrow^{K_{AB}} B}}{B \models A \leftrightarrow^{K_{AB}} B}$$

$$\frac{B \models B \leftrightarrow^{K_{BS}} S, \quad B \lhd \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}}{B \models S \mid\sim A \leftrightarrow^{K_{AB}} B}$$

$$\frac{}{B \models \text{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}$$

Herangehensweise: „von unten“

$$\frac{B \models S \Rrightarrow A \leftrightarrow^{K_{AB}} B, \quad \frac{\frac{\cdots}{B \models \mathrm{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}, \quad \frac{\cdots}{B \models S \mid\!\sim A \leftrightarrow^{K_{AB}} B}}{B \models S \models A \leftrightarrow^{K_{AB}} B}}{B \models A \leftrightarrow^{K_{AB}} B}$$

$$\frac{B \models B \leftrightarrow^{K_{BS}} S, \quad B \lhd \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}}{B \models S \mid\!\sim A \leftrightarrow^{K_{AB}} B}$$

$$\frac{B \models S \Rrightarrow \mathrm{fresh}\left(A \leftrightarrow^{K_{AB}} B\right), \quad \frac{}{B \models S \models \mathrm{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}}{B \models \mathrm{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}$$

Herangehensweise: „von unten“

$$\frac{B \models S \Rrightarrow A \leftrightarrow^{K_{AB}} B, \quad \frac{\frac{\dots}{B \models \text{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}, \quad \frac{\dots}{B \models S \mid\sim A \leftrightarrow^{K_{AB}} B}}{B \models S \models A \leftrightarrow^{K_{AB}} B}}{B \models A \leftrightarrow^{K_{AB}} B}$$

$$\frac{B \models B \leftrightarrow^{K_{BS}} S, \quad B \lhd \{A \leftrightarrow^{K_{AB}} B\}_{K_{BS}}}{B \models S \mid\sim A \leftrightarrow^{K_{AB}} B}$$

$$\frac{B \models S \Rrightarrow \text{fresh}\left(A \leftrightarrow^{K_{AB}} B\right), \quad \frac{B \models \text{fresh}\left(\dots\right), \; B \models S \mid\sim \text{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}{B \models S \models \text{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}}{B \models \text{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)}$$

Konsequenz

Wir brauchen $B \models \text{fresh}\left(\text{fresh}\left(A \leftrightarrow^{K_{AB}} B\right)\right)$!

Also: B muss *Nonce* schon *vor* dem Erzeugen von K_{AB} festlegen und hinterher überprüfen.

Ablauf: geändertes Needham/Schroeder-Protokoll

1. $A \rightarrow B : A$ „Ich möchte mit dir kommunizieren.“
2. $B \rightarrow A : \{A, N_B\}_{K_{BS}}$ „Ok.“
3. $A \rightarrow S : A, B, N_A, \{A, N_B\}_{K_{BS}}$
4. $S \rightarrow A : \{N_A, B, K_{AB}, \{A, N_B, K_{AB}\}_{K_{BS}}\}_{K_{AS}}$
5. $A \rightarrow B : \{A, N_B, K_{AB}\}_{K_{BS}}$
6. $B \rightarrow A : \{N_B\}_{K_{AB}}$
7. $A \rightarrow B : \{N_B - 1\}_{K_{AB}}$

Beweis für neues Needham/Schroeder-Protokoll

Beweis.

Sei $X := A \leftrightarrow^{K_{AB}} B$, dann:

$$\dfrac{B \models S \Rrightarrow X, \quad \dfrac{\dfrac{B \models S \Rrightarrow \mathrm{fresh}(X), \quad \dfrac{B \models \mathrm{fresh}(\mathrm{fresh}(X)), \quad B \models S \mathrel{|\!\sim} \mathrm{fresh}(X)}{B \models S \models \mathrm{fresh}(X)}}{B \models \mathrm{fresh}(X)}, \quad \dfrac{B \models B \leftrightarrow^{K_{BS}} S, \quad B \lhd \{X\}_{K_{BS}}}{B \models S \mathrel{|\!\sim} X}}{B \models S \models X}}{B \models A \leftrightarrow^{K_{AB}} B}$$

□

Das war's!