STSAL - Partea I

May 8, 2023

1 Subiectul I

$\varphi := S \triangleleft \{X\}_K$ and $\Psi := S \mid\equiv X$, give an example of BAN formula Γ such that Ψ can be inferred from $\Gamma \bigcup \{\varphi\}$.

2 Subiectul II

1. $I \rightarrow R : \{\{K_2\}_{sk(I)}\}_{K_1}$
2. $R \rightarrow I : \{"STLS", R, n_R\}_{K_2}$
3. $I \rightarrow R : \{I, n_R\}_{K_2}$

2.1 Idealizare

P1. $R \triangleleft \{\{R \overset{K_2}{\longleftrightarrow} I\}_{K_I{}^{-1}}\}_{K_1}$

P2. $I \triangleleft \{"STLS", n_R\}_{K_2}$

P3. $R \triangleleft \{n_R\}_{K_2}$

2.2 Asumptii

A1. $R \mid\equiv (R \overset{K_1}{\longleftrightarrow} I)$

A2. $R \mid\equiv \overset{K_I}{\longmapsto} B$

A3. $R \mid\equiv \#(R \overset{K_2}{\longleftrightarrow} I)$

A4. $R \mid\equiv (I \Rightarrow (R \overset{K_2}{\longleftrightarrow} I))$

A5. $R \mid\equiv \#(n_R)$

A6. $I \mid\equiv \#(n_R)$

A7. $I \mid\equiv (R \overset{K_2}{\longleftrightarrow} I)$

2.3 Demonstratie

1. $R \triangleleft \{R \overset{K_2}{\longleftrightarrow} I\}_{K_I{}^{-1}}$, din [SC3: A1, P1]
2. $R \mid\equiv I \mid\sim (R \overset{K_2}{\longleftrightarrow} I)$, din [MM-PK: A2, 1]
3. $R \mid\equiv I \mid\equiv (R \overset{K_2}{\longleftrightarrow} I)$, din [NV: A3, 2]
4. $R \mid\equiv (R \overset{K_2}{\longleftrightarrow} I)$, din [JR: A4, 3]
5. $R \mid\equiv I \mid\sim nR$, din [MM-SK: 4, P3]
6. $R \mid\equiv I \mid\equiv nR$, din [NV: A5, 5] - QED
7. $I \mid\equiv R \mid\sim ("STLS", n_R)$, din [MM-SK: A7, P2]
8. $I \mid\equiv R \mid\sim n_R$, din [BC4: 7]
9. $I \mid\equiv R \mid\equiv n_R$, din [NV: A6, 8]

3 Subiectul 3

3.1 Detalierea actiunilor

- $I \to R : I, R$
- $R \to S : I, R$
- $I \to R : \{I, pk(I)\}_{sk(S)}$
- $R \to I : \{R, n_R\}_{sk(S)}$
- $I \to R : \{n_R, I\}_{sk(I)}$
- $claim(I, R, recent - alive)$

- $send_1(I, R, (I, R))$
- $recv_1(R, I, (I, R))$
- $send_2(R, S, (I, R))$
- $recv_1(S, R, (I, R))$
- $send_3(S, R, \{I, pk(I)\}_{sk(S)})$
- $recv_3(R, S, \{I, pk(I)\}_{sk(S)})$
- $send_4(R, I, \{R, n_R\}_{sk(R)}$
- $recv_4(I, R, \{R, V\}_{sk(R)}$
- $send_5(I, R, \{V, I\}_{sk(R)}$
- $recv_5(R, I, \{n_R, I\}_{sk(R)}$
- $claim_6(I, R, recent - alive)$

3.2 Specificarea rolurilor

- $send_1(I, R, (I, R))$
- $recv_1(R, I, (I, R))$
- $send_2(R, S, (I, R))$
- $recv_1(S, R, (I, R))$
- $send_3(S, R, \{I, pk(I)\}_{sk(S)})$
- $recv_3(R, S, \{I, pk(I)\}_{sk(S)})$
- $send_4(R, I, \{R, n_R\}_{sk(R)}$
- $recv_4(I, R, \{R, V\}_{sk(R)}$
- $send_5(I, R, \{V, I\}_{sk(R)}$
- $recv_5(R, I, \{n_R, I\}_{sk(R)}$
- $claim_6(I, R, recent - alive)$

- $P(I) = \{(\{pk(I), sk(I), pk(R), pk(S)\},$
  $send_1(I, R, (I, R));$
  $recv_4(I, R, \{R, V\}_{sk(R)}$
  $send_5(I, R, \{V, I\}_{sk(R)}$ $)\}$