SOFTWARE SECURITY | WINTER TERM 2018/2019

SAFE AND SECURE SOFTWARE SYSTEMS
BTU COTTBUS-SENFTENBERG

Exercise Sheet 2: Protocol verification

Brandenburgische Technische Universität Cottbus - Senftenberg

[redacted]
Siddique Reza Khan
[redacted]

Kerberos Protocol:

1. First-order Goals
   - A believes $A \overset{K_{AB}}{\longleftrightarrow} B$
   - B believes $A \overset{K_{AB}}{\longleftrightarrow} B$

2. Second-Order Goals.
   - A believes B believes $A \overset{K_{AB}}{\longleftrightarrow} B$
   - B believes A believes $A \overset{K_{AB}}{\longleftrightarrow} B$,

Step1: Specify an idealized protocol variant

1. $S \rightarrow A: \{(T_S, A \overset{K_{AB}}{\longleftrightarrow} B, \{(T_S, A \overset{K_{AB}}{\longleftrightarrow} B)\}_{K_{BS}})\}_{K_{AS}}$
2. $A \rightarrow B: (\{(T_S, A \overset{K_{AB}}{\longleftrightarrow} B)\}_{K_{BS}}, \{(T_A, A \overset{K_{AB}}{\longleftrightarrow} B)\}_{K_{AB}})$
3. $B \rightarrow A: \{(T_A, A \overset{K_{AB}}{\longleftrightarrow} B)\}_{K_{AB}}$

Step2: specify necessary assumptions:

A1: A believes $A \overset{K_{AS}}{\longleftrightarrow} S$

A2: B believes $B \overset{K_{BS}}{\longleftrightarrow} S$

A3: S believes $A \overset{K_{AB}}{\longleftrightarrow} B$

A4: S believes $B \overset{K_{BS}}{\longleftrightarrow} S$

A5: S believes $A \overset{K_{AB}}{\longleftrightarrow} B$

A6: A believes (S controls $A \overset{K_{AB}}{\longleftrightarrow} B$)

A7: B believes (S controls $A \overset{K_{AB}}{\longleftrightarrow} B$)

A8: A believes fresh(T_S)

A9: B believes fresh(T_S)

A10: B believes fresh(T_A)

A11: A believes fresh(T_A)

Deduction rules:

R_1: $\dfrac{P \text{ believes } Q \overset{K}{\leftrightarrow} P,\ P \text{ sees } \{X\}_K}{P \text{ believes } Q \text{ said } X}$

R_2: $\dfrac{P \text{ believes fresh } X}{P \text{ believes fresh } (X, Y)}$

R_3: $\dfrac{P \text{ believes fresh } X,\ P \text{ believes } Q \text{ said } X}{P \text{ believes } Q \text{ believes } X}$

R_4: $\dfrac{P \text{ believes } Q \text{ believes } (X, Y)}{P \text{ believes } Q \text{ believes } Y}$

R_5: $\dfrac{P \text{ believes } Q \text{ controls } X,\ P \text{ believes } Q \text{ believes } X}{P \text{ believes } X}$

R_6: $\dfrac{P \text{ sees } (X, Y)}{P \text{ sees } X}$

R_7: $\dfrac{P \text{ sees } (X, Y)}{P \text{ sees } Y}$

Step 3: Proof for the first Protocol step

1.) A see $\{(T_S, A \xleftrightarrow{K_{AB}} B, \{(T_S, A \xleftrightarrow{K_{AB}} B)\}_{K_{BS}}\}_{K_{AS}}$

A believes $A \xleftrightarrow{K_{AS}} S$ (A1)

with R1,

A believes S said $(T_S, A \xleftrightarrow{K_{AB}} B, \{(T_S, A \xleftrightarrow{K_{AB}} B)\}_{K_{BS}})$

A believes fresh T_S (A8)

With R3, freshness nonce verification rule, before apply R2

A believes S believes $(T_S, A \xleftrightarrow{K_{AB}} B, \{(T_S, A \xleftrightarrow{K_{AB}} B)\}_{K_{BS}})$

$\Rightarrow$ decompose with R4

A believes S believes $A \xleftrightarrow{K_{AB}} B$

A believes S believes $(T_S, A \xleftrightarrow{K_{AB}} B)$

A believes S contrds $A \xleftrightarrow{K_{AB}} B$ (A6)

A believes S controls $(T_S, A \xleftrightarrow{K_{AB}} B)$ (A6)

$\Rightarrow$ with R5 jurisdiction rule

A believes $A \xleftrightarrow{K_{AB}} B$

Step 4: Proof of the Second Protocol step

2.) $A \rightarrow B : (\{T_S, A \xleftrightarrow{K_{AB}} B\}_{K_{BS}}, \{T_A, A \xleftrightarrow{K_{AB}} B\}_{K_{AB}})$

with R6,

B sees $\{T_S, A \xleftrightarrow{K_{AB}} B\}_{K_{BS}}$

B believes $B \xleftrightarrow{K_{BS}} S$ (A2)

With R1,

B believes S said $\{T_S, A \xleftrightarrow{K_{AB}} B\}$

B believes fresh T_S (A9)

With R2, before apply R3

B believes S believes $\{T_S, A \xleftrightarrow{K_{AB}} B\}$

B believes S controls $A \xleftrightarrow{K_{AB}} B$ (A7)

With R4, before apply R5

B believes $A \xleftrightarrow{K_{AB}} B$

B sees $\{T_A, A \xleftrightarrow{K_{AB}} B\}K_{AB}$ – from the message after applying R7

With R1,

B believes A said $\{T_A, A \xleftrightarrow{K_{AB}} B\}$

B believes fresh T_A (A10)

With R2, before apply R3

B believes A believes $\{T_A, A \xleftrightarrow{K_{AB}} B\}$

With R4,

B believes A believes $\{A \xleftrightarrow{K_{AB}} B\}$