# Exercise for Engineering Secure Software Systems

January 21, 2021: Exercises 8, 9

Henning Schnoor

Institut für Informatik, Christian-Albrechts-Universität zu Kiel

# Oral Exam

## date

- Tuesday, February 23
  - 9:30-12:30
  - 13:30-16:00
- each exam: $\approx 25$ minutes

## what to expect?

- questions cover all lecture aspects
- theory lecture: precise formal knowledge of key definitions required for discussion
- sequence: definitions, results, proofs, alternatives, …

## preparation

- use available material: slides, notes, exercises
- “readiness indicator:” review questions

## organization

- oral exam via BigBlueButton
- registration until Sunday, February 14: `https://www-ps.informatik.uni-kiel.de/pruefungsanmeldung/`, access code: 1O1BIS

# Leftovers

# Exercise

### Task (Needham-Schroeder as Horn clauses)

Model the Needham-Schroeder protocol as Horn clauses and use this formalism to show that the protocol is insecure. To do this, first list the facts, Dolev-Yao deductions, protocol deductions and the target clause. Then, use logical inference to show that the protocol is in fact insecure. Do you see any limits or imprecisions in this approach?

# Discussion: Tasks for this week

# Exercise

### Task (ProVerif example I)

Consider the following protocol:

1. $A \rightarrow B$ $\quad \mathrm{enc}^{s}_{k_{AB}}(N_A)$
2. $B \rightarrow A$ $\quad [\mathrm{enc}^{s}_{k_{AB}}(N_B), N_A]$
3. $A \rightarrow B$ $\quad N_B$

Here, $k_{AB}$ is a long-term symmetric key shared by Alice and Bob. Is the protocol secure in the sense, that it can only be completed correctly if both Alice and Bob participate in the protocol run? Analyse the protocol “by hand” and using ProVerif.

**Note**: If you use the standard ProVerif **query attacker**(FAIL) modeling, you need to express the “participation property” as secrecy property. We will study a different method using events later in the lecture.

# Exercise

### Task (ProVerif example II)

Choose a cryptographic protocol and use ProVerif to analyze its security properties, that is:

1. Specify the protocol in ProVerif (including the required cryptographic primitives),
2. specify the security property in ProVerif,
3. run ProVerif to search for attacks. Does the result match with your expectations?

You can use any protocol you find interesting—all the protocols mentioned in the course so far are good candidates. The following is an incomplete list:

- your modeling of the WhatsApp authentication protocol in the first exercise,
- the (broken) authentication protocols presented in the first exercise class and their fixes,
- the Needham-Schroeder(-Lowe) protocol,
- the Woo-Lam protocol,
- the ffgg protocol,
- the repaired version of the handshake-protocol from the ProVerif tutorial (the broken version was discussed in the lecture).

# Needham Schroeder Horn Representation

# Logic Modeling Outline

facts

- $d(\hat{k}_C)$
- $d(\{0,1\})$
- $\dots$

DY deductions

- $d(\mathrm{enc}^{\mathrm{a}}_{k_C}(x)) \wedge d(\hat{k}_C) \rightarrow d(x)$
- $d(x) \wedge d(y) \rightarrow d([x,y])$
- $d(x) \rightarrow d(\mathrm{hash}\,(x))$
- $\dots$

protocol deductions

- $d(\mathrm{enc}^{\mathrm{a}}_{k_B}([A,x])) \rightarrow d(\mathrm{enc}^{\mathrm{a}}_{k_A}([B,x]))$
- $d(\mathrm{enc}^{\mathrm{a}}_{k_A}([B,x,y])) \rightarrow (\mathrm{enc}^{\mathrm{a}}_{k_B}(y))$
- $\dots$

Horn clauses

$$(x_1 \wedge x_2 \wedge \cdots \wedge x_n \rightarrow y) \quad \leftrightarrow \quad (\overline{x_1} \vee \overline{x_2} \vee \cdots \vee \overline{x_n} \vee y)$$

target clause

$\neg d(\mathrm{FAIL})$

# Needham-Schroeder as Horn Clauses

as before

- Dolev-Yao clauses
- keys: $d\left(\epsilon, k_A, k_B, k_C, \hat{k}_C, \mathrm{BREAK}\right)$
- security: $\neg d(\mathrm{FAIL})$

protocol (w/Charlie)

$$\begin{array}{lllll} \text{Alice} & \epsilon & \rightarrow & \mathrm{enc}^{a}_{k_C}(A, N_A) \\ & \mathrm{enc}^{a}_{k_A}(N_A, y) & \rightarrow & \mathrm{enc}^{a}_{k_C}(y) \\ \text{Bob} & \mathrm{enc}^{a}_{k_B}(A, x) & \rightarrow & \mathrm{enc}^{a}_{k_A}(x, N_B) \\ & (\mathrm{BREAK}, N_B) & \rightarrow & \mathrm{FAIL} \end{array}$$

Horn translation

- A1: $d(\epsilon) \rightarrow d(\mathrm{enc}^{a}_{k_C}(A, N_A))$
- A2: $d(\mathrm{enc}^{a}_{k_A}(N_A, y)) \rightarrow d(\mathrm{enc}^{a}_{k_C}(y))$
  (what is $y$? **∀-quantified**!)
- B: $d(\mathrm{enc}^{a}_{k_B}(A, x)) \rightarrow d(\mathrm{enc}^{a}_{k_A}(x, N_B))$
  ($x$ is ∀-quantified)

attack: Adversary has

$\hat{k}_C$, BREAK, $\epsilon$, $\mathrm{enc}^{a}_{k_C}(A, N_A)$, $(A, N_A)$, $\mathrm{enc}^{a}_{k_B}(A, N_A)$, $\mathrm{enc}^{a}_{k_A}(A, N_B)$, $\mathrm{enc}^{a}_{k_C}(N_B)$, $N_B$, $(\mathrm{BREAK}, N_B)$, FAIL