# Exercise for Engineering Secure Software Systems

December 3, 2020: Exercises 3, 4

Henning Schnoor

Institut für Informatik, Christian-Albrechts-Universität zu Kiel

# Leftovers

# Exercise

**Task (minimal derivation properties)**

In the video lecture on the computation of the Dolev-Yao closure, we proved a lemma characterizing shortest derivations.

1. Can you generalize this result to handle signatures, MACs, and hash functions?
2. Which properties does the modeling of cryptographic primitives have to satisfy for an analog of this result to hold?
3. Can you come up with a modeling of cryptographic primitives where this property does not hold?

# Exercise

**Task (DY algorithm correctness)**

Prove that the algorithm for computing the DY closure (in its decisional variant **DERIVE**) as stated in the lecture is correct and runs in polynomial time. As in the lecture, restrict yourself to terms without applications of hash functions, signatures, or message authentication codes (MACs).

# Discussion: Tasks for this week

# Exercise

**Task (Formal Representation of the Woo Lam Protocol)**

Study the authentication protocol by Woo and Lam (see slide 17 of the lecture from November 10).

1. Specify the protocol as sequence of receive/send actions, once in the intended execution between Alice and Bob, and once in a form that allows to model the attack introduced in the lecture.
2. Specify the attack on the protocol formally.
3. How can we modify the protocol in order to prevent this attack?

# Exercise

**Task (Otway Rees Protocol)**

Consider the following protocol (Otway-Rees-Protocol):

1. $A \to B \quad [M, A, B, \mathrm{enc}^{\mathrm{s}}_{k_{AS}}([N_a, M, A, B])]$
2. $B \to S \quad [M, A, B, \mathrm{enc}^{\mathrm{s}}_{k_{AS}}([N_a, M, A, B]), \mathrm{enc}^{\mathrm{s}}_{k_{BS}}([N_b, M, A, B])]$
3. $S \to B \quad [M, \mathrm{enc}^{\mathrm{s}}_{k_{AS}}([N_a, k_{AB}]), \mathrm{enc}^{\mathrm{s}}_{k_{BS}}([N_b, k_{AB}])]$
4. $B \to A \quad [M, \mathrm{enc}^{\mathrm{s}}_{k_{AS}}([N_a, k_{AB}])]$
5. $A \to B \quad \mathrm{enc}^{\mathrm{s}}_{k_{AB}}(\mathrm{FAIL})$

1. Why are the subterms $M$, $A$, and $B$ in the second message sent both encrypted and as plaintext?
2. Why is the nonce $N_b$ encrypted in message 2?
3. Is the protocol secure? (You do not need to give a formal proof of security or insecurity.)

# Exercise

**Task (Security Modeling Issues: Are we Missing Something?)**

In the lecture, we defined security of a protocol as, essentially, unreachability of a state in which the adversary learns the constant FAIL. However, this FAIL-constant obviously does not have a correspondance in a real implementation of a protocol. In particular, the rules releasing the FAIL-constant are removed from the protocol in a real implementation. As a consequence, a potential security proof of a protocol in our formal model treats a different protocol than the protocol running in a real implementation.

Are there cases where this difference results in an insecure protocol that can be proven secure in our formal model? If this is the case, how can we circumvent this issue?

# Woo-Lam Protocol

# Example: Woo-Lam Authentication Protocol

## prerequisites

$k_{AS}$, $k_{BS}$: symmetric keys shared between Alice (Bob) and Server

## protocol

1. $A \to B \quad A$
2. $B \to A \quad N_B$
3. $A \to B \quad \mathrm{enc}^{\mathrm{s}}_{k_{AS}}(N_B)$
4. $B \to S \quad \mathrm{enc}^{\mathrm{s}}_{k_{BS}}\left([A, \mathrm{enc}^{\mathrm{s}}_{k_{AS}}(N_B)]\right)$
5. $S \to B \quad \mathrm{enc}^{\mathrm{s}}_{k_{BS}}(N_B)$

## idea

- only Alice can encrypt $N_B$ with $k_{AS}$
- server can check correctness

## issues?

- server is “decryption oracle”
- Alice does not “know” that she “talks to Bob”

## reference

Thomas Y. C. Woo and Simon S. Lam. “Authentication for Distributed Systems”. In: Computer 25.1 (Jan. 1992), pp. 39–52. ISSN: 0018-9162. DOI: 10.1109/2.108052. URL: http://dx.doi.org/10.1109/2.108052

# Woo-Lam Protocol is insecure

protocol

1. $A \to B \quad A$
2. $B \to A \quad N_B$
3. $A \to B \quad \mathrm{enc}^{s}_{k_{AS}}(N_B)$
4. $B \to S \quad \mathrm{enc}^{s}_{k_{BS}}\left([A, \mathrm{enc}^{s}_{k_{AS}}(N_B)]\right)$
5. $S \to B \quad \mathrm{enc}^{s}_{k_{BS}}(N_B)$

analysis

- **trash**: result of decrypting $\mathrm{enc}^{s}_{k_{CS}}(N_B)$ with $K_{AS}$
- $B$ believes $A$ participated in protocol run
- assumptions?

attack: $C$ controlled by $\mathcal{A}$, $B$ honest