CHRISTIAN-ALBRECHTS-UNIVERSITÄT ZU KIEL
Institut für Informatik · AG Software Engineering

Priv.-Doz. Henning Schnoor

Engineering Secure Software Systems Winter 2020/21
Exercise Sheet 2

issued: November 10, 2020 **due:** November 19, 2020

Exercise 2.1, simple example protocol (10 Points)

We consider the following simple authentication protocol:

- Alice sends a message M to Bob, together with her name A,
- Bob answers with a Nonce N_b,
- Alice answers with the term $\mathsf{sig}_{k_A}([M, B, N_B])$.

Please answer the following questions:

1. What are the security properties guaranteed by the protocol?
2. What is the purpose of the nonce N_B? What happens if we omit it?
3. What happens if the B is removed from Alice's last message?

Exercise 2.2, Fixing Broken Authentication Protocols (10 Points)

Consider the two authentication protocols presented in the exercise class:

a)

1. $A \rightarrow B \quad (A, \mathsf{enc}^{\mathsf{a}}_{k_B}(N_A))$
2. $B \rightarrow A \quad (B, \mathsf{enc}^{\mathsf{a}}_{k_A}(N_A))$

b)

1. $A \rightarrow B \quad (\mathsf{enc}^{\mathsf{a}}_{k_B}(N_A), \mathsf{enc}^{\mathsf{a}}_{k_B}(A))$
2. $B \rightarrow A \quad (\mathsf{enc}^{\mathsf{a}}_{k_A}(N_A, N_B), \mathsf{enc}^{\mathsf{a}}_{k_A}(B))$

Both of these protocols can be attacked with a similar attack as the Needham-Schroeder protocol or the example protocol we covered in the first exercise class. Suggest changes to the protocols that address these problems, and argue why you think your revised versions of the protocols are secure. Be as specific as possible in what "secure" means in this case.