Network Security
Summer 2015
Exercise 2

Prof. Dr.-Ing. Matthias Hollick
Secure Mobile Networking Lab — SEEMOO
https://www.seemoo.de

Goal

The goal of this exercise is to discuss several common mistakes that may occur when designing cryptographic protocols. After completing this exercise, you should be able to spot and avoid obvious flaws when applying cryptography to network security problems. There are of course numerous and much more complex ways in which a proposed protocol can violate its stated security goals. However, this is not a course on protocol verification, so only some very basic examples are discussed.

Deadline

The hard deadline for this exercise is **Wednesday 6th May, 2015, 23:00:00**. Late submissions are subject to the following penalty: (1) up to 1 day late: you will obtain 50 % of the achieved points; (2) up to 2 days late: you will obtain 25 % of the achieved points; (3) more than 2 days late: you will obtain zero points.

Bonus system

We decided to install a credit-based bonus system in our course. We will hand out credits in certain exercises if you (the students) deliver first-rate performance. Within the relevant exercises we will document the detailed requirements to obtain the bonus. Throughout the entire course 280 credits can be obtained in our bonus system. If you score at least 230 credits, you are eligible for a 0.7 grade bonus in the final exam. If you score between 190 and 229 credits, you are eligible for a 0.3 grade bonus. Below 190 credits we will not issue any bonus. Within this exercise, up to *10 bonus credits* can be obtained.

Protocol Assumptions and Definitions

The following protocol is started by an entity called Alice for mutually authenticating with another entity called Bob. After protocol execution has completed succesfully (i.e. no participant has preliminary aborted the execution), Alice and Bob have the following assumptions:

a) Alice assumes to be communicating with Bob.

b) Bob assumes to be communicating with Alice.

c) The key $K = K_1 || K_2$ is a shared secret between Alice and Bob (concatenation of Alice's key K_1 and Bob's key K_2).

For the protocol analysis, a few global definitions are necessary:

d) Only Dolev Yao Attackers are considered. This means that the attacker can intercept every message exchanged between the protocol participants. He decides whether to pass it on to the intended receipient as it is, or whether to reroute it to a different user, drop or manipulate it in any way he wishes ("god on the wire"). Injecting completely new messages is also possible.
He however cannot break any cryptographic primitives. If he wants to access encrypted data, he needs to know the key. If he wants to forge a signed message, he also needs the respective key.

e) Participants can start an arbitrary number of parallel sessions with other participants. It is legitimate to abort a session using a special ABORT message. Of course, an aborted session cannot lead to a successful authentication.

f) The connection is an open communication network. Participants only know the contents of messages, they do not have any meta information. This especially means that they are not able to determine who actually sent a certain message if it cannot be derived from the content of the message.

g) Nonces cannot be distinguished from keys. Both keys and nonces are equally distributed random data of the same length.

h) N denotes a nonce (a random number used once to ensure message freshness).

i) $\{x\}_k$ denotes a message x encrypted with key k; $\{x\}_k$ has the same length as x.
K is a symmetric key, B is B's public key, A is A's public key.

Problem 2.1 A Broken Authentication Protocol (Bonus: 10 Points)

Analyze the following protocol:

$A \rightarrow B : \{N_A\}_B, \{K_1\}_B$

$B \rightarrow A : N_A, \{N_B\}_A, \{K_2\}_A$

$A \rightarrow B : N_B$

Task 1: Determine which of the stated security goals (the assumptions Alice and Bob have after a successful execution of the protocol) can be violated if a Dolev Yao Attacker C is present on the communication channel. In other words: What can C achieve that he should not be able to? Write down the necessary protocol interaction.

Task 2: Propose a solution to fix the protocol so that your attack is no longer possible.

Task 3: In a practical implementation of authentication protocols it should be easy for the receiver to determine the authentic sender of the message. Modify the proposed authentication protocol or your solution of Task 2 in a secure way to deal with this requirement. You are able to add additional messages or additional information to the existing messages. Feel free to use crypto if you want.