University of Stuttgart
Institute of
Information Security

Grundlagen der Informationssicherheit
Winter Term 2017/18
Prof. Dr. Ralf Küsters

Homework 6

Submission into the *green SEC mailbox* in front of Room 2.041 until January 30, 2018, 17:30.

General Notes

- If you encounter difficulties, you SHOULD[1] ask the teaching assistants in the tutorial sessions.
- To solve the homework, you SHOULD form teams of 3 people.
- Your team size MUST NOT exceed 3 people.
- You MUST submit your homework on paper (one submission per team).
- You are free to choose whether you write your solutions in German or in English.
- If your submission contains multiple sheets, you MUST staple them.
- Each sheet of your submission MUST include all team member's names and matriculation numbers.
- If you do not adhere to these rules, you risk loosing points.

Problem 1: Protocol for Mutual Authentication (5 points)

The goal of the protocol given below is to mutually authenticate two communication partners. The protocol assumes that both parties, A and B, share a secret symmetric encryption key k. As usual N_A and N_B denote nonces (generated by A or B respectively).

$$\begin{array}{lllll} 1. & A \to B & : & enc_k^s(N_A) \\ 2. & B \to A & : & enc_k^s(N_B), N_A \\ 3. & A \to B & : & N_B \end{array}$$

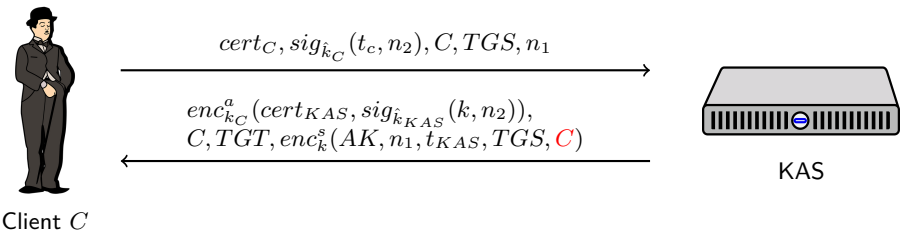
Find an attack on the protocol in which A runs multiple sessions of the protocol while B does not participate at all. One of these sessions must complete successfully. Draw a figure that shows the message flow of your attack. Explain the underlying problem in 2–3 sentences.

Problem 2: Kerberos (5 points)

As we have seen in the lecture, the Public-Key-Kerberos protocol is vulnerable to a MitM attack. As a result of this attack, the client receives the tokens TGT and AK that have been issued for the attacker's account.

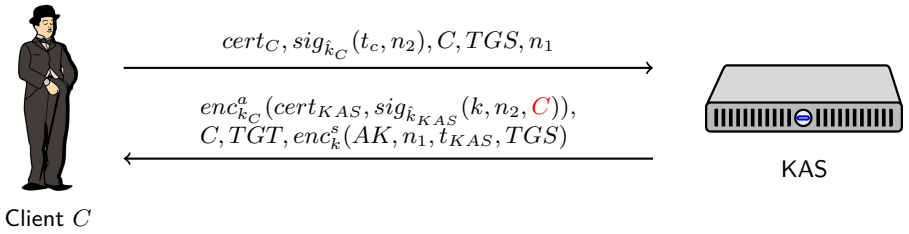
In the following, we will look at three approaches to fix this problem. Decide for each approach whether it prevents MitM attacks similar to the one presented in the lecture. Explain why the respective approach fixes / does not fix the underlying problem (in not more than 2–3 sentences each).

(a)

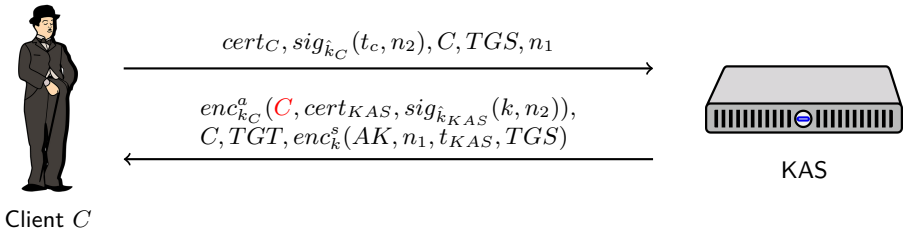


[1] SHOULD, MUST, and MUST NOT are used as defined in RFC2119.

(b)



(c)



Remark: It is possible that all or none of the above fix the problem.

Problem 3: TLS and Randomness (5 points)

As generating random numbers is expensive, one might be tempted to re-use randomness when connecting to the same communication partner several times. In TLS a client might want to re-use N_C and PMS when connecting to the same server for a second time. (The client will still choose fresh values when connection to a different server for the first time.)

Show that this approach is insecure by finding an attack where

- the client runs multiple TLS handshakes with the same server,
- all handshakes finish successfully on the client's side, and
- there is at least one handshake in which the actual server did not participate.

Draw a figure that shows the message flow of your attack. Explain in 2–3 sentences why this attack is possible.

Problem 4: Attack on IKEv1 Main Mode ★ (5 points) bonus

In the lecture, we have seen an attack on the aggressive mode of IKEv1 (using a pre-shared symmetric key). For the main mode of IKEv1 (using a pre-shared symmetric key), there is a similar attack. Draw a figure that shows the message flow of this attack. Explain in 2–3 sentences why this attack is possible.

Hint: The attacker does not need to start a session for this attack (in contrast to the attack on the aggressive mode).

Remark: IKE will be covered in the lecture in the week after this homework sheet has been published. Therefore, the points of this problem are bonus points.