Brandenburg University of Technology
Cottbus-Senftenberg
Chair of IT Security

Exercise Class
"Introduction into Cyber Security"
Winter Term 2018/2019

Introduction into Cyber Security
– 9th Exercise Sheet –

Discussion on: 23th January 2019

Topics

This exercise deals with the continuation of the discussion of authentication schemes, especially the Needham-Schroeder Protocol and the Kerberos Protocol. Further we will repeat some basics about asymmetric key cryptography especially elliptic curves.

Instructions

The exercise sheets are to be worked on by you in self-study. In the exercise classes, usually only the control / discussion of the solutions takes place. The following preparation is therefore obligatory:

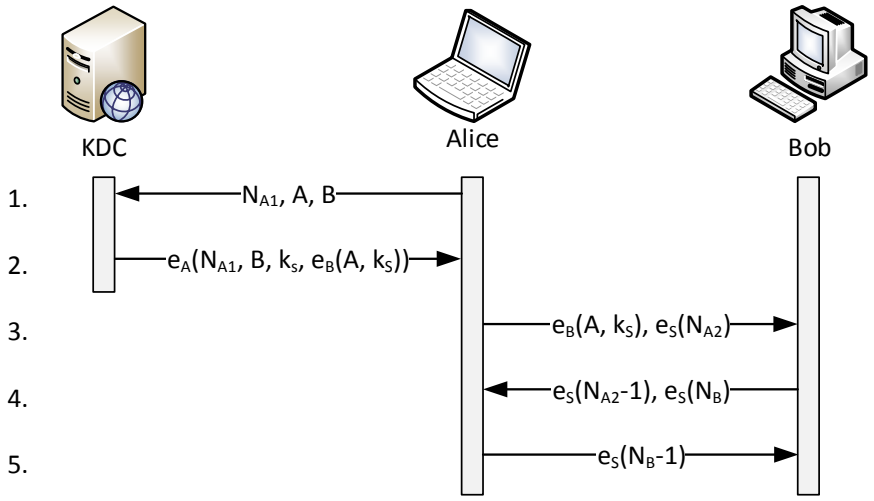
1. Read the exercise sheet with the tasks carefully. In case you have questions, please resolve them in advance with the tutor or your fellow students.

2. Use the lecture slides to repeat the content of the current subject and check your knowledge.

Careful preparation and processing of the exercise sheets (in addition to attending the lecture) is an essential prerequisite for success in the final exam.

Task 1: Needham-Schroeder Protocol (cont.)

a) For all protocol messages shown in the figure, explain the purpose of the respective elements in the message!

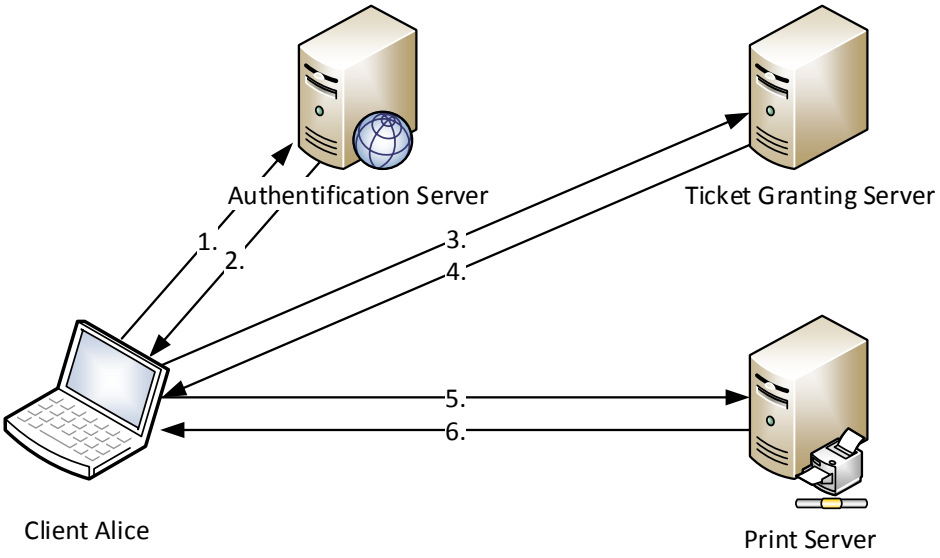


b) Explain the problem of replay attacks in the symmetric protocol variant.

c) Suppose the used nonces are 64 bit long and DES ECB mode is used for there encryption. Find an attack on the protocol.

Task 2: Kerberos Protocol

a) Use the illustration to explain the processes of Kerberos! Explain all protocol messages and create a reference to the scenario from task 1 (The Needham-Schroeder protocol).



b) What is the purpose of the ticket granting server in the Kerberos protocol?

c) What are Kerberos' (practical) advantages over Needham-Schroeder?

d) Which Kerberos vulnerabilities and security deficiencies have been identified?

Task 3: Repetition on Elliptic Curve Cryptography

We consider the following simple ECC Cryptoscheme, where a message m should be send as a point P_m: (x,y) on the curve. It is the point P_m that will be encrypted.

1. Repeat the basics of elliptic curves (Definition, Addition operation, Geometrical interpretation).

2. Why we can not simply encode the message m as the x,y coordinates of P_m?

3. Have you an idea how one could encode the message m for the usage of elliptic curve cryptography?

Lets assume that the algorithm works in the following way:

For an given elliptic curve $E : y^2 = x^3 + \alpha x + \beta$ over $\mathbb{F}_q$, q prime, and an given point $G \in E$ each user selects an private key n_{user} and generates a public key $P_{\text{user}} = n_{\text{user}} \times G$. To encrypt and send a message P_m to an user B, the user A chooses a random positive integer k and calculates the cypher-text C_m as the set of two points $C_m = \{kG, P_m + kP_B\}$. To decrypt the cypher-text, B multiplies the first point, kG, by its private key n_B and subtracts the result from the second point. The user B obtains $P_m + kP_B - n_B(kG)$.

1. Proof that the encrypted message from B equals P_m.

2. Which knowledge and possibilities has an possible attacker?