Brandenburg University of Technology
Cottbus-Senftenberg
Chair of IT Security

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

Introduction into Cyber Security
– 8th Exercise Sheet –

Discussion on: 16th January 2019

Topics

This exercise deals with the Internet key exchange protocol, the secured transport layer (TLS) and the topic web-security in general. In the exercise itself we will discuss/present the third practical task about web-security.

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: IPsec/IKE and NAT

1. Why does not IKE work for connections over Network Address Translation (NAT)? How can this issue be solved?

2. Let there are two NAT devises behind a security gateway. The two NAT devices assign the same local address to two different machines. What problem will occur at the gateway when both machines run IPsec with NAT-T? How would you address this problem?

Task 2: IKE

1. What is the difference between IKE_SA and CHILD_SA?

2. In case of IKE authentication exchange, why do we also exchange (SA_i1, TS_i, TS_r) and (SA_r2, TS_i, TS_r) in the AUTH payload?

3. Explain why man in the middle is not possible in IKE?

Task 3: Transport Layer Security (TLS)

1. In SSL/TLS, why is there a separate Change Cipher Spec Protocol rather than including a `change_cipher_spec` message in the Handshake Protocol?

2. What purpose does the MAC serve during the change cipher spec TLS exchange?

3. What are the security goals associated with TLS? Consider the following threats and describe how each is countered by a particular feature of TLS.

    a) Brute-force attack: exhaustive search of the key space for a conventional encryption algorithm.

    b) Known plaintext dictionary attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary for these known plaintexts and tries to determine the right key by reducing the possible keys with the interception of matching ciphertexts.

    c) Replay attack: Earlier TLS handshake messages are replayed.

    d) Man-in-the-Middle attack: An attacker interposes during key exchange.

    e) Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped.

Task 3: Non-Digital Authentication Examples

With the Needham Schroeder protocol (discussed in task 4) and Kerberos (discussed on next exercise sheet), so-called tickets are used. Construct a concrete scenario from the real (non-digital) world, which can serve as a metaphor for network authentication. In your scenario, there should be at least two tickets to certify the property statements.

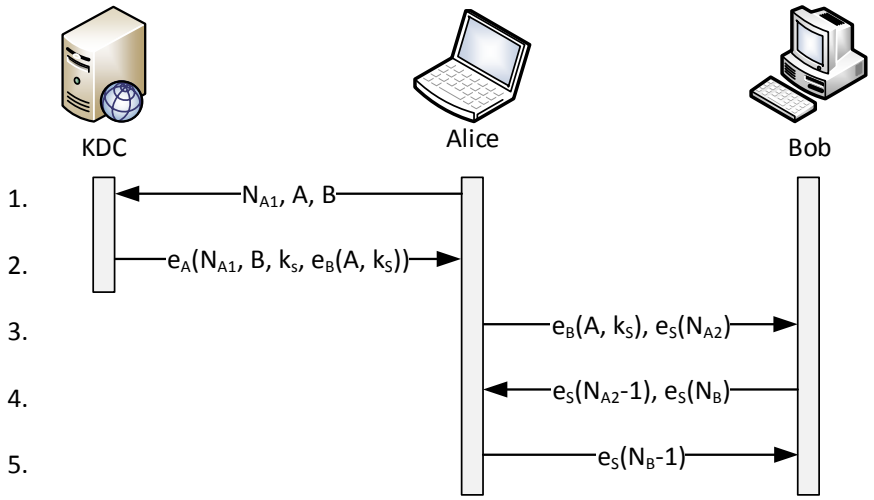
Hint: For instance, consider reduced prices or special authorizations for certain groups of people at events, e.g., student discount

a) Explain which “tickets” appear in your scenario.

b) Why are “tickets” being used? What would be disadvantages of a solution without “tickets”?

Task 4: Needham-Schroeder Protocol

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.