

## Homework 5

1. What can attacker that controls the network do to a communication between a client and a server?
2. Before starting a TCP connection, client and servers perform a three-way handshake. Describe how can this three-way handshake can be abused by an attacker?
3. Consider the following simple mutual authentication protocol:

$$\begin{aligned} A \rightarrow B: & N_a \\ B \rightarrow A: & \{N_a, N_b\}_{K_{ab}} \\ A \rightarrow B: & N_b \end{aligned}$$

Explain how an attacker  $B'$  can launch an impersonation attack by intercepting all messages for  $B$  and make  $A$  decrypt her own challenges.

4. What is the main problem with the following authentication protocol where  $A$  sends  $B$  mutually shared key?

$$A \rightarrow B : K_{AB}$$

5. Nonces are unpredictable random numbers used in protocols? Consider the following protocol

$$\begin{aligned} A \rightarrow B: & N \\ B \rightarrow A: & \{N + 1\}_{K_{ab}} \end{aligned}$$

Write down three facts that  $A$  can infer after this protocol has been successfully completed?

6. (**Deleted:** same as 2) Before starting a TCP connection, client and servers perform a three-way handshake:

$$\begin{aligned} A \rightarrow S: & \text{SYN} \\ S \rightarrow A: & \text{SYN-ACK} \\ A \rightarrow S: & \text{ACK} \end{aligned}$$

How can this protocol be abused causing trouble on the server?

7. Write down a protocol which establishes a secret key between  $A$  and  $B$  using a mutually trusted third party  $S$ . You can assume  $A$  and  $S$ , respectively  $B$  and  $S$ , share secret keys.
8. Consider the following protocol between a car and a key transponder:

- (a)  $C$  generates a random number  $r$
- (b)  $C$  calculates  $(F, G) = \{r\}_K$
- (c)  $C \rightarrow T: r, F$
- (d)  $T$  calculates  $(F', G') = \{r\}_K$
- (e)  $T$  checks that  $F = F'$
- (f)  $T \rightarrow C: r, G'$
- (g)  $C$  checks that  $G = G'$

In Step 2 and 4 a message is split into two halves. Explain what the purpose of this split is? Assume the key  $K$  is shared only between the car and the transponder. Does the protocol achieve that the transponder  $T$  authenticates itself to the car  $C$ ? Does the car authenticate itself to the transponder?