Homework 5

Please submit your solutions to the email address 7ccsmsen at gmail dot com. Please submit only ASCII text or PDFs. Every solution should be preceded by the corresponding question, like:

Qn**:**	**...a difficult question from me...**
A:	**...an answer from you ...**
Q$n+1$	**...another difficult question...**
A:	**...another brilliant answer from you...**

Solutions will only be accepted until 30th December!

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:

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

   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 unpredicatble random numbers used in protocols. Consider the following protocol

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

   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:

$$\begin{array}{ll} A \to S: & \text{SYN} \\ S \to A: & \text{SYN-ACK} \\ A \to S: & \text{ACK} \end{array}$$

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, respectfully B and S, share secret keys.

8. Consider the following protocol between a car and a key transponder:

   (a) C generates a random number N

   (b) C calculates $(F, G) = \{N\}_K$

   (c) $C \to T$: N, F

   (d) T calculates $(F', G') = \{N\}_K$

   (e) T checks that $F = F'$

   (f) $T \to C$: N, 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?