Homework 5

Please submit your solutions to the email address 7ccsmsen at gmail dot com. Please submit only one homework per email. Please also submit only ASCII text or PDFs (no .docs etc). 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 20th December! Submit with your partner a single solution!

1. Imagine you are researching security products (e.g. CCTV, alarms etc) on a helpful website. They ask you for your address details? Think about whether this can be bad for you.

2. What can attacker that controls the network do to a communication between a client and a server?

3. 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?

4. 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.

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

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

6. 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?

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 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?

9. What are the main disadvantages of the following protocol that establishes a mutual key between two parties A and B with the help of a mutually trusted third party S:

$$\begin{array}{ll} A \to S: & A, B \\ S \to A: & \{K_{AB}\}_{K_{AS}} \text{ and } \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}} \\ A \to B: & \{K_{AB}\}_{K_{BS}} \\ A \to B: & \{m\}_{K_{AB}} \end{array}$$

10. Explain briefly the purpose of the certification authority in the public-private key encryption scheme.

11. Explain briefly what is meant by a certification authority becoming "too big to fail" when it has issued a large number of certificates.

12. In which situations does it make sense to install invalid (self-signed) certificates?

13. **(Optional)** This question is for you to provide regular feedback to me, for example what were the most interesting, least interesting, or confusing parts in this lecture? Is there anything you like to have improved or explained in the handouts? Please feel free to share any other questions or concerns.