Security

Assignment 4, Friday, September 30, 2016

Handing in your answers: For the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2016/exercises.html`

To summarize:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Hans or Joost). When working together, include **both** your names and student numbers.
- Submit one single **pdf** file – when working together, only hand in **once**.
- Hand in via Blackboard, before the deadline.

Deadline: Monday, October 9, 09:00 sharp!

Goals: After completing these exercises successfully you should be able to

- analyze simple authentication protocols;
- discover and repair relay and reflection attacks.

Marks: You can score a total of 100 points.

Notation: In all of the exercises below, N_A and N_B are fresh random nonces generated by A and B, respectively, and K_{AB} is a shared secret key of A and B. A shared encryption key K_{AB} is assumed to be secure; that is, Eve cannot simply break it (not even by brute force).

1. **(30 points)** Alice and Bob share a key K_{AB} and want to use this key to communicate confidentially. They first carry out the following mutual-authentication protocol:

$$\begin{aligned} A \to B: &\quad \text{“I'm Alice. Let's talk”} \\ B \to A: &\quad N_B \\ A \to B: &\quad K_{AB}\{N_B\}, N_A \\ B \to A: &\quad K_{AB}\{N_A\} \end{aligned}$$

   After this authentication phase they communicate and encrypt their messages M as $K_{AB}\{M\}$.

   (a) How can Eve authenticate as Alice towards Bob? Use arrow notation to describe the communication! Note that Eve does not necessarily need to initiate the protocol.

   (b) How can Eve obtain a valid ciphertext $K_{AB}\{M\}$ of a message M of her choice? Again, use arrow notation!

   (c) What simple measure prevents the second attack?

. . . . . **The assignment continues on the next page!** . . . . . .

2. **(30 points)** Alice (A) and Bob (B) are both trying to authenticate each other using a shared secret key (K_{AB}) only they know. Eve is trying to impersonate either Alice or Bob.

   In which of the following four authentication protocols can Eve impersonate Alice or Bob by using a replay attack? Recall that in a replay attack, Eve records a message sent by Alice or Bob (while possibly preventing that message from reaching the addressee) and at any later point in time retransmits this recorded message.

   For the vulnerable protocols write down the attack, using the '$E(A) \longrightarrow B : message$' notation (for E impersonating A, by sending *message* to B). Clearly say which message an attacker stores and replays. If not, *explain why a replay attack would fail.*

   Note that a replay attack is *not* the same as a man-in-the-middle attack!

   (a)
   $$\begin{array}{lllll} 1. & A \longrightarrow B & : & hello \\ 2. & B \longrightarrow A & : & B, K_{AB}\{B\} \\ 3. & A \longrightarrow B & : & A, K_{AB}\{A\} \end{array}$$

   (b)
   $$\begin{array}{lllll} 1. & A \longrightarrow B & : & A, K_{AB}\{N_A\} \\ 2. & B \longrightarrow A & : & B, N_A, K_{AB}\{N_B\} \\ 3. & A \longrightarrow B & : & A, B, N_A, N_B, K_{AB}\{N_A, N_B\} \end{array}$$

   (c)
   $$\begin{array}{lllll} 1. & A \longrightarrow B & : & A, N_A, K_{AB}\{A, N_A\} \\ 2. & B \longrightarrow A & : & B, N_B, K_{AB}\{B, N_A, N_B\} \\ 3. & A \longrightarrow B & : & K_{AB}\{A, B, N_A\} \end{array}$$

   (d)
   $$\begin{array}{lllll} 1. & A \longrightarrow B & : & A, N_A \\ 2. & B \longrightarrow A & : & B, N_B, K_{AB}\{B, N_A - 1\} \\ 3. & A \longrightarrow B & : & K_{AB}\{A, B, N_B + 1\} \end{array}$$

3. **(40 points)** Consider the following two flawed mutual authentication protocols.

   $$(i) \left\{ \begin{array}{lllll} A & \longrightarrow & B & : & A, N_A \\ B & \longrightarrow & A & : & N_B, K_{AB}\{N_A + 3\} \\ A & \longrightarrow & B & : & K_{AB}\{N_B + 6\} \end{array} \right. \qquad (ii) \left\{ \begin{array}{lllll} A & \longrightarrow & B & : & A, K_{AB}\{N_A - 1\} \\ B & \longrightarrow & A & : & N_A, K_{AB}\{N_B - 1\} \\ A & \longrightarrow & B & : & K_{AB}\{A, B, N_A\} \end{array} \right.$$

   In this exercise we are *not* interested in man-in-the-middle attacks, only reflection or replay attacks.

   (a) Show that protocol (i) is flawed in the sense that an attacker Eve (E) can pretend to be Alice (A). Use the protocol attack notation $E(A) \longrightarrow B : m$.

   (b) Fix protocol (i) by modifying only one message.

   (c) Show that also protocol (ii) is flawed – in the sense that an attacker Eve (E) can pretend to be Alice (A).

   (d) Fix protocol (ii) by, once again, only modifying one message.