Security

Assignment 4, Wednesday, September 30, 2015

Handing in your answers: the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2015/exercises.html`

Briefly,

- submission via Blackboard (`http://blackboard.ru.nl`);
- one single pdf file;
- make sure to write all names and student numbers and the name of your teaching assistant (Brinda or Joost).

Deadline: Thursday, October 8, 24:00 (midnight) sharp!

Goals: After completing these exercises successfully you should

- understand message freshness and its relation to authenticity;
- be able to discover and repair relay and reflection attacks in authentication protocols

Marks: You can score a total of 100 points.

1. **(30 points)** Consider the following two protocols for a "remote keyless system" (e.g., a remote car-door opener):

   - The remote sends K_{AB} to the car, the car opens if and only if a received string is K_{AB}.
   - The remote has an internal counter c, the car has an internal counter c'; those are set to the same starting value during production. Each time the remote opens the car it sends $K_{AB}(c)$ and increases c by 1; the car opens if and only if the received value equals $K_{AB}(c')$ and increases c' after opening.

   (a) Why is the first protocol insecure? Describe an attack; use arrow notation!

   (b) For the second protocol, describe an attack that a third party could perform to break availability.

   (c) In the lecture slides, challenge-response protocols were described that could be used here instead. What kind of special functionalities would that require the remote to have (both cryptographic and otherwise)? Why would some manufacturers still use the above method, instead?

2. **(40 points)** Alice (A) and Bob (B) are both trying to authenticate each other using a shared secret key (K_{AB}) only they know.

   Eve (E) is trying to impersonate either Alice or Bob, that is, making Alice or Bob believe that he/she is communicating with the other party while in fact they are communicating with Eve. To achieve this, Eve can actively influence the communication channel between Alice and Bob by deleting, modifying and inserting messages. In a *replay attack*, in particular, 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.

   In which of the following four authentication protocols can Eve impersonate Alice or Bob by using a replay attack? 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). If not, explain why a replay attack would fail. In case of a replay attack, clearly say which message an attacker stores and replays.

   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. The shared encryption key K_{AB} is assumed to be secure; that is, Eve cannot simply break it (not even by brute force).

   (a)
   1. $A \longrightarrow B \quad : \quad hello$
   2. $B \longrightarrow A \quad : \quad B, K_{AB}\{B\}$
   3. $A \longrightarrow B \quad : \quad A, K_{AB}\{A\}$

(b)
1. $A \longrightarrow B \;:\; A, K_{AB}\{N_A\}$
2. $B \longrightarrow A \;:\; B, N_A, K_{AB}\{N_B\}$
3. $A \longrightarrow B \;:\; A, B, N_A, N_B, K_{AB}\{N_A, N_B\}$

(c)
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. $A \longrightarrow B \;:\; K_{AB}\{A, B, N_A\}$

(d)
1. $A \longrightarrow B \;:\; A, N_A$
2. $B \longrightarrow A \;:\; B, N_B, K_{AB}\{B, N_A - 1\}$
3. $A \longrightarrow B \;:\; K_{AB}\{A, B, N_B + 1\}$

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

$$(i)\begin{cases} A \longrightarrow B \;:\; A, N_A \\ B \longrightarrow A \;:\; N_B, K_{AB}\{N_A + 2\} \\ A \longrightarrow B \;:\; K_{AB}\{N_B + 4\} \end{cases} \qquad (ii)\begin{cases} A \longrightarrow B \;:\; A, K_{AB}\{N_A - 1\} \\ B \longrightarrow A \;:\; N_A, K_{AB}\{N_B - 1\} \\ A \longrightarrow B \;:\; K_{AB}\{A, B, N_A\} \end{cases}$$

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.