Security

Assignment 5, Friday, October 13, 2017

Handing in your answers:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Bart 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 23, 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;
- work with different modes of operation for block ciphers;
- recognize and avoid pitfalls of these modes.

Marks: You can score a total of 100 points.

1. **(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 '$E(A) \longrightarrow B : \mathit{message}$' 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)
   1. $A \longrightarrow B : \mathit{hello}$
   2. $B \longrightarrow A : B, K_{AB}\{B\}$
   3. $A \longrightarrow B : A, K_{AB}\{A\}$

   (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. $A \longrightarrow B : K_{AB}\{A, B, N_B + 1\}$

The assignment continues on the next page!

2. **(30 points)** Consider the following two flawed mutual authentication protocols.

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

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

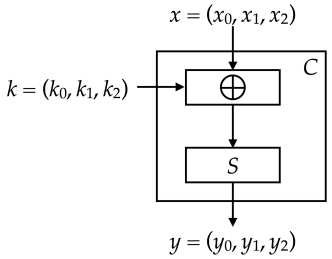
(a) Show that protocol (i) is flawed in the sense that an attacker Eve (E) can pretend to be Alice (A). Use the protocol attack notation $E(A) \longrightarrow B : m$.

(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.

3. **(20 points)** Assume a block cipher C that encrypts a plaintext block x using a key k.



S:

Plaintext	Ciphertext
000	001
001	000
010	011
011	110
100	010
101	111
110	100
111	101

In particular, C maps a 3-bit input block $x = (x_0, x_1, x_2)$ to a 3-bit output block $y = (y_0, y_1, y_2)$ using a 3-bit key $k = (k_0, k_1, k_2)$ and a function S as follows:

$$y = C(x, k) = S(x_0 \oplus k_0, x_1 \oplus k_1, x_2 \oplus k_2),$$

where S is the substitution described above.

So, for instance encrypting `001` with key `101` becomes $C(001, 101) = S(100) = 010$ and decrypting `100` with key `110` becomes $C^{-1}(100, 110) = S^{-1}(100) \oplus 110 = 110 \oplus 110 = 000$.

(a) Compute the ciphertext belonging to plaintext `011 111 101 001` (so, using blocks of three bits) with key $k =$ `101` using Electronic Code Book (ECB) mode. Show intermediate steps.

(b) Do the same for Cipher Block Chaining (CBC) mode, where the Initialisation Vector (IV) is `111`. Show intermediate steps.

(c) Give at least one reason why CBC mode is preferred over the ECB mode.

4. **(20 points)** In this exercise, we will take a look at the counter mode (CTR). We use the same block cipher C that was introduced in the previous exercise.

(a) Assume that the key $k =$ `101`, and $IV =$ `100`. Compute the first 9 bits of key stream. Show intermediate computations! *Hint:* interpret the IV as a 3-bit binary number.

(b) Assume that the plaintext is `001 110 111`. Compute the matching ciphertext.

(c) While CTR is generally a great choice, there is one pitfall: an IV should never be repeated. Assume you have a plaintext $p_1 =$ `010 110 110` and a corresponding ciphertext $c_1 =$ `110 001 101`, for a certain unknown key and IV, as well as a different ciphertext $c_2 =$ `101 011 111` that was obtained by encrypting p_2 with the same key and IV. Compute the matching plaintext p_2. Show your computations!