Security

Assignment 11, Monday, December 5, 2011

Handing in your answers: There are two options:

1. Put your solutions in Pim's post box (in the white cabinet, lower door, near the printer at the station-side-end of the corridor on the second floor of the Huygens building). Before handing in, make sure:
   - your names and student numbers are written on the document.
2. Send your solutions by e-mail to `pim@cs.ru.nl` with subject '*assignment 11*'. This e-mail should only contain a single PDF document as attachment. Before handing in, make sure:
   - your names and student numbers are included in the document (since it will be printed),
   - your names are part of the filename (example: PimVullers_FlavioGarcia-11.pdf), and
   - the file is a PDF document.

Deadline: Monday, December 12, 8:30 sharp!

Note: Do not forget to perform the modulo operations.

1. **(4 points)** Alice wants to communicate with Bob and wants to be sure he is really Bob.
   (a) Consider that they use a Public Key Infrastructure (PKI) based on a hierarchical tree structure where Certificate Authorities (CA's) issue digital certificates by signing them with their private key. To convince Alice, Bob sends a certificate to her that states his public key and is signed by CA X. However, Alice has never heard of X before, describe the steps that she needs to take to verify (the validity of) this certificate.
   (b) An alternative would be that they use a crowd-based PKI in which Bob sends, for example, his PGP public key (or key ID) to Alice. Describe, again, what Alice needs to do to verify (the validity of) this public key. Focus on the differences and similarities with the previous approach.
2. **(4 points)** Consider the ElGamal signature scheme, see Wikipedia[1]. Suppose $G = \mathbb{Z}_p^*$ for $p = 29$, with generator $g = 3$ and secret number $n = 21$.
   (a) Determine the corresponding h.
   (b) Sign the message $m = 15$ using ElGamal signatures. We will use the hash function $H(x) = x$ and random value $r = 5$.
      i. Compute $s_1 = g^r \mod p$.
      ii. Compute $r^{-1} \mod p - 1$.
      iii. Compute $s_2 = (H(m) - n \cdot s_1) \cdot r^{-1} \mod (p - 1)$
   (c) Verify that the signature is correct using h.
3. **(2 points)** Consider a system with key distribution using a central server S. The system uses tickets to reduce the workload of the server and to simplify re-authentication. The first protocol is used to establish a shared secret key, which is used for authentication, and to exchange the ticket (explanation below):

[1] `http://en.wikipedia.org/wiki/ElGamal_signature_scheme`

1. $A \longrightarrow B \;:\; N_A, A$
2. $B \longrightarrow S \;:\; N_A, A, N_B, B$
3. $S \longrightarrow B \;:\; K_{BS}\{N_B, A, K_{AB}\}, K_{AS}\{N_A, B, K_{AB}\}$
4. $B \longrightarrow A \;:\; K_{AS}\{N_A, B, K_{AB}\}, K_B\{T, A, K_{AB}\}, N'_B, K_{AB}\{N_A\}$
5. $A \longrightarrow B \;:\; K_{AB}\{N'_B\}$

When Alice wants to contact Bob she sends him a nonce N_A and her name A. Bob requests a secret key at the server by forwarding this information together with his own nonce N_B and name B. The server chooses a key K_{AB} and encrypts it, together with the name of the other and their own nonce, for both Alice (using K_{AS}, the key shared with Alice) and Bob (using K_{BS}). The server sends both ciphertexts to Bob, who decrypts his own ciphertext. Using his personal secret key K_B he constructs a ticket, containing a timestamp T, the key K_{AB} and the name A. Then he sends Alice's ciphertext, the ticket, a new nonce N'_B and Alice's nonce encrypted under the key K_{AB} that is to proof that he knows this key. Alice decrypts the ciphertext from the server and learns the key, which she uses to verify the encrypted nonce sent by Bob. Finally she sends Bob's new nonce encrypted using K_{AB} to show that she also knows the key. Now Alice and Bob have mutually authenticated each other.

When, in the future, Alice wants to re-authenticate with Bob she can use the ticket in the second protocol. Now, she only has to send the ticket and perform a simple challenge-response protocol to verify that they both still know the key:

1. $A \longrightarrow B \;:\; N'_A, K_B\{T, A, K_{AB}\}$
2. $B \longrightarrow A \;:\; N''_B, K_{AB}\{N'_A\}$
3. $A \longrightarrow B \;:\; K_{AB}\{N''_B\}$

Your task is to find an attack on this system which allows an evil attacker E to authenticate to Bob (that is, impersonating Alice).