Model Exam Question H0N21A Introduction to ICT Security

Part on Cryptology (Bart Preneel)

26 December 2014

Recommendation on how to use this model exam. Study the course, analyze the protocol carefully, think thoroughly about the definitions and about each answer and write them down. Go through the questions and answers a second time, because the answer to a subsequent question may change your views. Only then should you check the answers on the next page.
If something is not clear, do not hesitate to ask me questions.

The following protocol has been proposed by ICAO to verify the authenticity of a passport A and a passport reader B.

Alice A **Bob** B

$$\xleftarrow{\quad cert B \quad}$$

$$\xrightarrow{\quad \alpha^a \bmod p \,||\, r_A \quad}$$

$$\xleftarrow{\quad \alpha^y \bmod p \,||\, \mathrm{Sig}_B(r_A || \alpha^y \bmod p) \quad}$$

Here one has the following definitions:

- p a prime number
- α a generator mod$p$
- A the identity of Alice and B the identity of Bob
- r_A a random string generated by Alice
- a the private key of A
- $\alpha^a \bmod p$ the public key of A
- y an integer chosen uniformly at random with $1 < y < p - 1$.
- $\mathrm{Sig}_X(.)$ signature with the private key S_X of X
- $certX$ a certificate of a third party on the public key of X

a) How can Alice and Bob agree on a session key?

b) Does this protocol achieve entity authentication from Alice to Bob and from Bob to Alice? Motivate your answer.

c) Does this protocol achieve implicit key authentication from Alice to Bob and from Bob to Alice? Motivate your answer.

d) Does this protocol provide key confirmation from Alice to Bob and from Bob to Alice? Motivate your answer.

e) Does this protocol offer forward secrecy? Motivate your answer.

f) Does this protocol resist a known (session) key attack? Motivate your answer.

Answer to the previous questions.

a) How can Alice and Bob agree on a session key?
Answer: Bob computes $k = (\alpha^a)^y \bmod p$ and Alice computes $k = (\alpha^y)^a \bmod p$. (Note that it would be even better to compute the hash value of $\alpha^{ay} \bmod p$.)

b) Does this protocol achieve entity authentication from Alice to Bob and from Bob to Alice? Motivate your answer.
Answer. Note that the definition of entity authentication is often not completely understood; please look it up carefully and do not forget the "liveliness" aspect.
The protocol does not provide entity authentication of Alice to Bob since Alice only sends her public key and a random number – hence Bob cannot know that Alice is actively present.
The protocol provides entity authentication of Bob to Alice since Alice sends in step 2 a fresh challenge r_B and Bob returns in step 3 a signature on this challenge (computed with his private signing key).

c) Does this protocol achieve implicit key authentication from Alice to Bob and from Bob to Alice? Motivate your answer.
Answer. Note that the definition of implicit key authentication is often misunderstood. Implicit key authentication from Alice to Bob means: does Bob know that Alice is the only party who can possibly obtain the session key? Similarly from Bob to Alice.
The protocol provides implicit key authentication of Alice to Bob *if Bob has an authenticated copy of Alice's public key, e.g., through a certificate.* In that case Bob knows that only Alice can find the session key. Without an authenticated copy of Alice's public key, the property does not hold.
The protocol provides implicit key authentication of Bob to Alice since from the signature in the third message Alice learns that Bob has generated $\alpha^y \bmod p$; from this Alice can deduce that Bob is the only other party who can compute the session key.

d) Does this protocol provide key confirmation from Alice to Bob and from Bob to Alice? Motivate your answer.
Answer. There is no key confirmation; Alice does not know that her message has arrived correctly and Bob does not know that his second message (third step) has arrived correctly. Moreover, even if those messages have arrived, the parties do not know from each other that they have performed the Diffie-Hellman key calculation correctly.

e) Does this protocol offer forward secrecy? Motivate your answer.
Answer. No. If Alice's long term secret key a leaks, an opponent who has stored all past interactions can deduce the session key for each of those interactions. If Bob's long term secret key leaks, there is no problem.

f) Does this protocol resist a known (session) key attack? Motivate your answer.
Answer. If someone would obtain a session key, it would not be possible to make the parties reuse the key. The reason is that an attacker could replay the value $\alpha^y \bmod p$ in the third message, but the signature cannot be replayed: it contains the fresh random number r_A just sent by Alice; this allows Alice to detect a replay.