SECURITY IN NETWORKED COMPUTING SYSTEMS

February 06 , 2017

Name _____ **Serial nr.** _____

EXERCISE NO. 1 #MARKS: 10

With reference to the RSA scheme, where *d* and *e* are the private and public exponents respectively,

1. Illustrate the square-and-multiply algorithm for modular exponentiation and discuss its performance;
2. In the light of point 1, argue why the usual choice for public exponent *e* is either 3 or $2^{16}+1$;
3. Argue whether the same optimization can be done on private exponent *d*;

EXERCISE NO. 2 #MARKS: 12

A client *C* and a server *S* share a password Π. Furthermore, client *C* knows the public key PK_S of server *S*. Client and server are equipped with computationally secure hash functions, symmetric and asymmetric ciphers. Finally, client and server clocks are not synchronized. Under these assumptions, client and server attempt to establish a symmetric session key K_{CS} by means of the following key establishment protocol:

$$\begin{array}{lll} M1 & C \rightarrow S: & E_{PK_S}(C, S, n_c, \Pi, K_{CS}) \\ M2 & S \rightarrow C: & E_{K_{CS}}(S, C, n_c, n_s) \\ M3 & C \rightarrow S: & n_s \end{array}$$

where the kind of encryption scheme, symmetric or asymmetric, is clear from the context.

1. Argue whether the protocol satisfies the confidentiality of the password Π in the case of *ciphertext-only* attack.
2. Assume now the adversary gets hold of a session key $\overline{K_{cs}}$ and records the protocol instance $\{\overline{M1}, \overline{M2}, \overline{M3}\}$ that led to that key establishment.
    a. Argue whether the confidentiality of password Π is still guaranteed under this assumption (hint: considers an off-line guessing attack).
    b. Argue whether the protocol suffers from a replay attack.
    c. If the protocol suffers from any of these attacks, modify it in order to prevent them.

EXERCISE NO. 3 #MARKS: 8

a. Introduce the main fields of a certificate.
b. When is a certificate invalid?
c. When is a certificate revoked?

Solution

Exercise #1

See theory.

Exercise #2

Question #1.

The protocol guarantees confidentiality of the password because it is transmitted in its encrypted form. Furthermore, M1 is randomized so that an exhaustive data search is not feasible.

Question #2a.

Confidentiality is not guaranteed anymore because the adversary can obtain n_c from M2. Now the adversary knows fields C, S, n_c and K_{CS} of this message and thus can use message M1 to mount an off-line password attack against Π.

Question #2b.

The protocol is subject to replay attack because S has no proof of the freshness of message M1. Therefore, if an adversary has obtained a session key $\overline{K_{cs}}$ and the related protocol messages$\{\overline{M1}, \overline{M2}, \overline{M3}\}$, then the adversary can mount a replay attack by performing the following steps:

1. Initially, the adversary replays message $\overline{M1}$ so making the server S to reuse key $\overline{K_{cs}}$;
2. Then the adversary completes the key establishment protocol using key $\overline{K_{cs}}$.

Question #2c.

The protocol can be redesigned as follows:

$$\begin{array}{lll} M1 & S \rightarrow C: & n_s \\ M2 & C \rightarrow S: & E_{PK_S}(C, S, n_c, n_s, \Pi, K_{CS}) \\ M3 & S \rightarrow C: & E_{K_{CS}}(S, C, h(n_c)) \end{array}$$

where quantity n_s proves *S* the freshness of message M2. Furthermore, quantity $h(n_c)$ proves *C* that *S* knows n_c without revealing n_c. Thus, the adversary cannot exploit this knowledge in an off-line guessing attack of the password based on M2. Notice that the adversary knows n_s which is transmitted in the clear.

Exercise #3

See theory

Question a.

I expect that the candidate *at least* talks about the following fields: i) identifier of the certificate holder, ii) period of validity, iii) public key and iv) digital signature computed on the previous fields.