HW #3 - CNS Sapienza

Daniele Oriana 1457625

26 Nov 2015

20120709-Q3

Q3.1 Describe the original Needham-Schroeder scheme, its vulnerability and its fixing.
Q3.2 Describe a one-way authentication scheme based on X509 certificates and discuss what guarantees it ensures.

Answer

Q3.1

NeedhamSchroeder is a protocol that allows the mutual authentication between two entities through a mechanism based on public key cryptography. The most important feature of this mechanism is the introduction of a third party, called trusted authority, which ensures the correct correspondence between a public key and an entity. In examining the steps that make up the protocol we use the following notation:

- K_{PX} represents the public key of X
- Sig_C is the digital signature of C (trusted authority that guarantees public keys)

The protocol is based on the following steps (we suppose that the authentication involves A (Alice) and B(Bob)):

- Alice sends to C: <I'm Alice and i want to talk with Bob> (<A,B>)
- C replies to Alice with : <B, K_{PB}, Sig_C(K_{PB}, B)>
- Alice checks the digital signature of C, generates a nonce N and sends to Bob: K_{PB}(N,A)

- Bob now decodes the message sended by A and starts the same steps done by A, in fact Bob sends to C: <I'm Bob and i want to talk with Alice> <(B,A)>
- C replies to Bob with : <B, K_{PA}, Sig_C(K_{PA}, A)>
- Bob now checks the digital signature of C, generates a nonce N' and sends to Alice K_{PB}(N,N')
- A finally decodes the message sended by Bob and replies sending K_{PB}(N') to Bob

The protocol described is insecure, in fact it presents a vulnerability that allows a critical attack. We suppose that an attacker (we call it Trudy and we refer to it as T) is a system user that, being authenticated, can talk to A, B and C; we suppose also that this attacker can induce Alice to start an authentication session with him. Trudy can exploit the vulnerability realizing an attack that is a combination of man in the middle and reflection attack. The attack is done in this way:

- Alice generates a nonce N and sends to Trudy a message encrypted with Trudy's public key K_{PT} which contains the pair N, Alice's identifier
- Trudy receives the message, decrypts it and sends to Bob the pair N,Alice'identifier encrypted with the public key of Bob K_{PB}
- Bob generates a nonce N' and then sends to Trudy a message encrypted with the public key of Alice K_{PA} which contains the pair N,N'
- Trudy can't decode the message, therefore she forwards it to Alice
- Alice decodes the message with her private key and checks N. If the control is fine then Alice has authenticated Trudy. Then Alice sends to Trudy a message encrypted with the public key of Trudy that contains N'
- Trudy decodes the message with her private key obtaining N', then encrypts it with Bob's public key and sends it to him

At the end of these steps Trudy is authenticated to Bob as Alice. We have to note that Trudy acts between Alice and Bob transparently, as is typical in MITM, she also starts two simultaneous connections with Alice and Bob similar to what happens in the reflection attack.

The protocol can be easly solved introducing a little modification: in the third point of the procedure described previously Bob, instead of sending the pair N, N', sends the triple N, N', B; in this way, after the forwarding of Trudy, Alice can understand that something is wrong because she doesn't speaking with Bob.

Q3.2

In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). It is based on public key cryptography and digital signatures, in addiction it provides three different types of authentication protocols: One-Way,Two-Way and Three-Way. With X.509 one-way authentication we have a single transfer of information from A to B. In the usual scenario in which Alice and Bob are the two entities involved in the process, this one-way mode guarantees that: Alice generates the message and plays as the sender, Bob is the receiver, the integrity and the originality of the message is maintained. To provide these features the protocol uses:

- a timestamp $\mathrm{t_a}$
- a session key $\mathrm{K_{AB}}$ between Alice and Bob
- Bob's public key $\mathrm{P_B}$
- a certificate of Alice's public key certA signed by a certification authority.

For the authentication Alice presents to Bob the required credentials, sending them in one step:

certA, $\mathrm{t_a}$, Bob's identifier, $\mathrm{P_B(K_{AB})}$, $\mathrm{Sig_A}$($\mathrm{t_a}$, Bob's identifier, $\mathrm{P_B(K_{AB})}$).

The timestamp indicates the generation and expiration time, it is used to prevent delayed delivery of messaged. This process can also include a nonce, that is a random number; its value must be unique within the expiration time of the message and, through this nonce, B is able to detect replay attacks, storing the nonce and rejecting any new message with the same nonce.