Needham-Schroeder Public Key

Author(s): Roger Needham and Michael Schroeder December 1978
Submitted by Ralf Treinen November 4, 2002
Last modified December 9, 2002

Summary: Mutual authentication, using a trusted key server and public keys.

Protocol specification (in common syntax)

```
A,B,S :                    Principal
Na,Nb :                    Nonce
KPa,KPb,KPs,KSa,KSb,KSs :  Key
KPa,KSa :                  is a key pair
KPb,KSb :                  is a key pair
KPs,KSs :                  is a key pair
```

```
1.    A  ->  S   :    A,B
2.    S  ->  A   :    {KPb, B}KSs
3.    A  ->  B   :    {Na, A}KPb
4.    B  ->  S   :    B,A
5.    S  ->  B   :    {KPa, A}KSs
6.    B  ->  A   :    {Na, Nb}KPa
7.    A  ->  B   :    {Nb}KPb
```

Description of the protocol rules

This protocol has been proposed by [NS78]. In this protocol description, `KSa` (resp. `KSb`, `KSs`) is the secret key corresponding to the public key `KPa` (resp. `KPb`, `KPs`).

Requirements

After completion of the protocol, the two principals `A` and `B` should be convinced about the identity of their respective correspondent.

References

[NS78].

Claimed proofs

Burrows, Abadi and Needham [**?**] prove the correctness of the protocol in the sense of their logical framework. However, they point out a possible replay attack which, according to them, could be avoided by using timestamps.

Claimed attacks

An intruder `I` may impersonate `A`, by inciting `A` to initiate a second session[Low95]. In the following, we ignore the message exchanges with the public key server and only consider messages between the principals `A` and `B`, and the intruder `I`. We assume that the intruder `I` possesses a key pair `(KPi, KSi)`, and we may also assume that every principal knows the public keys `KPa`, `KPb` and `KPi`.

```
i.3.       A    ->    I     :    {Na,A}KPi
ii.3.    I(A)   ->    B     :    {Na,A}KPb
ii.6.      B    ->  I(A)    :    {Na,Nb}KPa
i.6.       I    ->    A     :    {Na,Nb}KPa
i.7.       A    ->    I     :    {Nb}KPi
ii.7.    I(A)   ->    B     :    {Nb}KPb
```

Remark

It has been proposed to fix the protocol by including the respondent's identity in the response [Low95].

See also

Lowe's fixed version of Needham-Schroder Public Key

Citations

[Low95] Gavin Lowe. An attack on the Needham-Schroeder public key authentication protocol. *Information Processing Letters*, 56(3):131–136, November 1995.

[NS78] Roger Needham and Michael Schroeder. Using encryption for authentification in large networks of computers. *Communications of the ACM*, 21(12), December 1978.