Lowe's fixed version of Needham-Schroder Public Key

Author(s): Gavin Lowe 1995
Last modified November 6, 2002

Summary: This protocol is an amended version of the Needham-Schroeder Public Key. Its purpose id mutual authentication, using a trusted keyserver 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, B}KPa
7.    A  ->  B   :    {Nb}KPb
```

Description of the protocol rules

Compared to the original version of the Needham-Schroeder Public Key protocol, the identity of the responder `B` has been added in the message `6` to prevent the attack discovered in [Low95].

Requirements

See Needham-Schroeder Public Key.

References

[Low95]

Claimed proofs

It is reported in [Low95] that the technique that permitted to find the Lowe attack on the Needham-Schroeder Public Key protocol (running FDR on a CSP presentation of the protocol) found no attack on this protocol.

See also

Needham-Schroeder 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.