Lowe modified Denning-Sacco shared key

Author(s): Gavin Lowe 1997
Last modified November 12, 2002

Summary: Modified version of the Denning-Sacco shared key protocol to correct a freshness flaw. Distribution of a shared symmetric key by a trusted server and mutual authentification. Symmetric key cryptography with server and timestamps.

Protocol specification (in common syntax)

```
A, B, S :        principal
Nb :             nonce
Kas, Kbs, Kab :  key
T :              timestamp
dec :            nonce -> nonce
```

```
1.    A  ->  S  :    A, B
2.    S  ->  A  :    {B, Kab, T, {Kab, A, T}Kbs}Kas
3.    A  ->  B  :    {Kab,A, T}Kbs
4.    B  ->  A  :    {Nb}Kab
5.    A  ->  B  :    {dec(Nb)}Kab
```

Description of the protocol rules

This version add a nonce handshake (messages 4, 5) at the end of Denning-Sacco shared key to prevent the attack from [Low97].

Requirements

See Needham Schroeder Symmetric Key.

References

[Low97]

See also

Needham Schroeder Symmetric Key, Denning-Sacco shared key.

Citations

[Low97] Gavin Lowe. A family of attacks upon authentication protocols. Technical Report 1997/5, Department of Mathematics and Computer Science, University of Leicester, 1997.