Lowe modified Wide Mouthed Frog

Author(s): Gavin Lowe 1997
Last modified November 20, 2002

Summary: An modified version of Wide Mouthed Frog. Exchanged of a fresh shared key. Symmetric key cryptography with server and timestamps.

Protocol specification (in common syntax)

```
A, S :            principal
Kas, Kbs, Kab :   symkey
Nb :              nonce
Ta, Ts :          timestamp
suc :             nonce -> nonce

1.   A  ->  S  :   A, {Ta, B, Kab}Kas
2.   S  ->  B  :   {Ts, A, Kab}Kbs
3.   B  ->  A  :   {Nb}Kab
4.   A  ->  B  :   {succ(Nb)}Kab
```

Description of the protocol rules

Two messages have been appened to Wide Mouthed Frog for mutual authentification of `A` and `B` (*nonce handshake*).

Remark

The two final messages were added by Lowe to the Wide Mouthed Frog protocol to prevent an attack claimed in [Low97] which actually fails against the complete original specification of the protocol in [BAN89], see Wide Mouthed Frog.

Requirements

See Wide Mouthed Frog.

References

[Low97]

See also

Wide Mouthed Frog

Citations

[BAN89] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. Technical Report 39, Digital Systems Research Center, february 1989.

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