Lowe modified BAN concrete Andrew Secure RPC

Author(s): Gavin Lowe 1996
Last modified November 14, 2002

Summary: A modified version of the BAN concrete Andrew Secure RPC protocol, preventing a parallel session attack. Exchanged of a fresh shared key, Symmetric key cryptography.

Protocol specification (in common syntax)

```
A, B :          principal
Kab, K'ab :     symkey
Na, Nb, N'b :   nonce
succ :          nonce -> nonce

1.    A  ->  B  :   A, Na
2.    B  ->  A  :   {Na, K'ab, B}Kab
3.    A  ->  B  :   {Na}K'ab
4.    B  ->  A  :   Nb
```

Description of the protocol rules

The identity of the responder `B` has been added in the message `2` of `andrewBAN2`.

Requirements

See Andrew Secure RPC.

References

[Low96]

See also

Andrew Secure RPC, BAN modified Andrew Secure RPC, BAN concrete Andrew Secure RPC.

Citations

[Low96] Gavin Lowe. Some new attacks upon security protocols. In IEEE Computer Society Press, editor, *In Proceedings of the Computer Security Foundations Workshop VIII*, 1996.