BAN concrete Andrew Secure RPC

Author(s): Michael Burrows and Martin Abadi and Roger Needham 1989
Last modified November 14, 2002

Summary: A concrete realization of the Andrew Secure RPC protocol, stronger and with less encryption. 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}Kab
3.   A  ->  B  :   {Na}K'ab
4.   B  ->  A  :   Nb
```

Description of the protocol rules

This protocol establishes the fresh shared symmetric key `K'ab`.

The nonce `Nb` is sent in message `4` to be used in a future session.

We assume that initially, the symmetric keys `Kab` is known only to `A` and `B`.

Requirements

See Andrew Secure RPC.

References

[BAN89]

Claimed attacks

In [Low96], with 2 parallel runs where the intruder `I` impersonates `B`.

```
i.1.      A    ->  I(B)   :   A, Na
ii.1.   I(B)   ->   A     :   B, Na
ii.2.     A    ->  I(B)   :   {Na, K'ab}Kab
i.2.    I(B)   ->   A     :   {Na, K'ab}Kab
i.3.      A    ->  I(B)   :   {Na}K'ab
ii.3.   I(B)   ->   A     :   {Na}K'ab
i.4.    I(B)   ->   A     :   Ni
ii.4.     A    ->  I(B)   :   Nb
```

A fix to this attack can be found in Lowe modified BAN concrete Andrew Secure RPC.

See also

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

Citations

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

[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.