BAN modified Andrew Secure RPC

Author(s): Michael Burrows and Martin Abadi and Roger Needham 1987
Last modified November 14, 2002

Summary: Modified version of Andrew Secure RPC correcting a freshness flaw. 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}Kab
2.    B  ->  A   :    {succNa, Nb}Kab
3.    A  ->  B   :    {succNb}Kab
4.    B  ->  A   :    {K'ab, N'b, Na}Kab
```

Description of the protocol rules

The nonce `Na` has been added to the message `4` of Andrew Secure RPC to prevent the flow presented in Andrew Secure RPC.

Requirements

See Andrew Secure RPC.

References

[BAN89]

See also

Andrew Secure RPC, BAN concrete 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.