Andrew Secure RPC

Author(s): M. Satyanarayanan 1987
Last modified November 14, 2011

Summary: 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}Kab
```

Description of the protocol rules

This protocol establishes the fresh shared symmetric key `K'ab`. The nonce `N'b` 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

The protocol must guaranty the secrecy of the new shared key `K'ab`: in every session, the value of `K'ab` must be known only by the participants playing the roles of `A` and `B`.

The protocol must guaranty the authenticity of `K'ab`: in every session, on reception of message `4`, `A` must be ensured that the key `K'ab` in the message has been created by `A` in the same session.

References

[Sat89]

Claimed attacks

[BAN89]. The message `4` contains nothing that `A` knows to be fresh. Hence, an intruder `I` can replay this message in another session of the protocol to convinced `B` to accept an old compromised key.

```
i.1.       A     ->    B     :    A, {Na}Kab
i.2.       B     ->    A     :    {succNa, Nb}Kab
i.3.       A     ->    B     :    {succNb}Kab
i.4.       B     ->    A     :    {K'ab, N'b}Kab
ii.1.      A     ->    B     :    A, {Ma}Kab
ii.2.      B     ->    A     :    {succMa, Mb}Kab
ii.3.      A     ->    B     :    {succMb}Kab
ii.4.      B     ->   I(A)   :    {K''ab, M'b}Kab
ii.4.     I(B)   ->    A     :    {K'ab, N'b}Kab
```

See also

BAN modified 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.

[Sat89] M. Satyanarayanan. Integrating security in a large distributed system. *ACM Transactions on Computer Systems*, 7(3):247–280, 1989.