Amended Needham Schroeder Symmetric Key

Author(s): Roger Needham and Michael Schroeder January 1987
Last modified November 8, 2002

Summary: This is an amended version of Needham Schroeder Symmetric Key, by the same authors. Distribution of a shared symmetric key by a trusted server and mutual authentification. Symmetric key cryptography with server.

Protocol specification (in common syntax)

```
A, B, S :        principal
Na, Nb :         number
Kas, Kbs, Kab :  key
dec :            number -> number

1.    A  ->  B  :    A
2.    B  ->  A  :    {A, Nb}Kbs
3.    A  ->  S  :    A, B, Na, {A, Nb}Kbs
4.    S  ->  A  :    {Na, B, Kab, {Kab, Nb, A}Kbs}Kas
5.    A  ->  B  :    {Kab, Nb, A}Kbs
6.    B  ->  A  :    {Nb}Kab
7.    A  ->  B  :    {dec(Nb)}Kab
```

Description of the protocol rules

See Needham Schroeder Symmetric Key. The extra exchange of the nonce `Nb` prevents the Denning Sacco freshness attack described in Needham Schroeder Symmetric Key.

Requirements

See Needham Schroeder Symmetric Key.

References

[NS87].

See also

Needham Schroeder Symmetric Key, Kerberos V5.

Citations

[NS87] R. Needham and M. Schroeder. Authentication revisited. *Operating Systems Review*, 21(7), January 1987.