Paulson's strengthened version of Yahalom

Author(s): Paulson 0, 2001
Last modified October 4, 2002

Summary: Paulson's modified version of the Yahalom protocol. Symmetric keys and trusted server.

Protocol specification (in common syntax)

```
A, B, S :        principal
Na, Nb :         number fresh
Kas, Kbs, Kab :  key

A knows :  A, B, S, Kas
B knows :  B, S, Kbs
S knows :  S, A, B, Kas, Kbs

1.   A  ->  B  :   A, Na
2.   B  ->  S  :   B, Nb, {A, Na}Kbs
3.   S  ->  A  :   Nb, {B, Kab, Na}Kas, {A, B, Kab, Nb}Kbs
4.   A  ->  B  :   {A, B, Kab, Nb}Kbs, {Nb}Kab
```

Description of the protocol rules

To prevent the attacks [Syv94] of to BAN simplified version of Yahalom protocol, the name of B has been added to the cipher sent by S in message 3 and transmitted by A in message 4.

Requirements

See Yahalom.

References

[Pau01]

Claimed proofs

[Pau01]

See also

Yahalom,
BAN simplified version of Yahalom

Citations

[Pau01] Lawrence C. Paulson. Relations between secrets: Two formal analyses of the yahalom protocol. *J. Computer Security*, 2001.

[Syv94] Paul Syverson. A taxonomy of replay attacks. In *Proceedings of the 7th IEEE Computer Security Foundations Workshop*, pages 131–136. IEEE Computer Society Press, 1994.