Yahalom

Author(s): Yahalom 0, 1988
Last modified October 4, 2002

Summary: Distribution of a fresh symmetric shared key by a trusted server and mutual authentication. 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, {A, Na, Nb}Kbs
3.   S  ->  A  :   {B, Kab, Na, Nb}Kas, {A, Kab}Kbs
4.   A  ->  B  :   {A, Kab}Kbs, {Nb}Kab
```

Description of the protocol rules

The fresh symmetric shared key Kab is created by the server S and sent encrypted, in message 3 both to A (directly) and to B (indirectly).

Requirements

The protocol must guaranty the secrecy of Kab: in every session, the value of Kab must be known only by the participants playing the roles of A, B and S.

A must be also properly authentified to B.

References

This version of the Yahalom protocol is the one found in [BAN89] (cited as personal communication in this paper).

It is also presented in [CJ97].

Claimed proofs

[BAN89], [Pau01]

See also

BAN simplified version of Yahalom,
Paulson's strengthened version of Yahalom.

Citations

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

[CJ97] John Clark and Jeremy Jacob. A survey of authentication protocol literature : Version 1.0., November 1997.

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