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)

\[ \begin{align*} 
A, B, S &: \text{ principal} \\
Na, Nb &: \text{ number fresh} \\
Kas, Kbs, Kab &: \text{ key} \\
A \text{ knows} &: A, B, S, Kas \\
B \text{ knows} &: B, S, Kbs \\
S \text{ knows} &: S, A, B, Kas, Kbs \\
1. A \rightarrow B &: A, Na \\
2. B \rightarrow S &: B, \{A, Na, Nb\}Kbs \\
3. S \rightarrow A &: \{B, Kab, Na, Nb\}Kas, \{A, Kab\}Kbs \\
4. A \rightarrow B &: \{A, Kab\}Kbs, \{Nb\}Kab \\
\end{align*} \]

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].

http://www.lsv.ens-cachan.fr/spore
Claimed proofs

[BAN89], [Pau01]

See also

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

Citations


http://www.lsv.ens-cachan.fr/spore