BAN simplified version of Yahalom

Author(s): Burrows Abadi Needham 0, 1989
Last modified October 9, 2002

Summary: An amended version of the Yahalom protocol, presented in the BAN logic paper. 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, Kab, Nb}Kbs
4.    A  ->  B  :     {A, Kab, Nb}Kbs, {Nb}Kab
```

Description of the protocol rules

Compared to the original version of the Yahalom protocol, the nonce `Nb` is added to the second cipher of message `3`, to prevent a malicious `A` to reuse an old value of `Kab`.

Also, `Nb` is sent in cleartext in message `2`, which makes possible the attacks below.

Requirements

See Yahalom.

References

This simplified version of the Yahalom protocol was proposed in [BAN89].

Claimed proofs

[BAN89]

Claimed attacks

Replay attack with interleaving and type error in [Syv94].

```
i.1.       A    ->  I(B)   :    A, Na
i.2.       B    ->  I(S)   :    B, Nb, {A, Na}Kbs
ii.1.    I(A)   ->   B     :    A, Na, Nb
ii.2.      B    ->  I(S)   :    B, Nb, {A, Na, Nb}Kbs
i.3.                       :    Omitted
i.4.     I(A)   ->   B     :    {A, Na, Nb}Kbs, {Nb}Na
```

In the message 1 of session ii, the pair Na, Nb is used as a nonce N'a, and in the last message of session i, Na is used as the key Kab.

A second replay attack is described in the same paper [Syv94].

```
i.1.        A    ->  I(B)   :    A, Na
ii.1.     I(B)   ->   A     :    B, Na
ii.2.       A    ->  I(S)   :    A, N'a, {B, Na}Kas
iii.1.                     :    Omitted
iii.2.    I(A)   ->   S     :    A, Na, {B, Na}Kas
iii.3.      S    ->  I(B)   :    Na, {A, Kab, Na}Kbs, {B, Kab, Na}Kas
i.2.                       :    Omitted
i.3.      I(S)   ->   A     :    Ni, {B, Kab, Na}Kas, {A, Kab, Na}Kbs
i.4.        A    ->  I(B)   :    {A, Kab, Na}Kbs, {Ni}Kab
```

See also

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.

[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.