Neumann Stubblebine

Author(s): B. Clifford Neumann and Stuart G. Stubblebine April 1993
Last modified November 8, 2002

Summary: Session key exchange inspired by the Yahalom protocol with the addition of timestamps, and mutual authentication. Symmetric key cryptography with server.

Protocol specification (in common syntax)

```
A, B, S :          principal
Na, Ma, Nb, Mb :   number
Kas, Kbs, Kab :    key
Ta, Tb :           time

1.    A  ->  B  :   A, Na
2.    B  ->  S  :   B, {A, Na, Tb}Kbs, Nb
3.    S  ->  A  :   {B, Na, Kab, Tb}Kas, {A, Kab, Tb}Kbs, Nb
4.    A  ->  B  :   {A, Kab, Tb}Kbs, {Nb}Kab
5.    A  ->  B  :   Ma, {A, Kab, Tb}Kbs
6.    B  ->  A  :   Mb, {Ma}Kab
7.    A  ->  B  :   {Mb}Kab
```

Description of the protocol rules

The messages `1-4` are the part concerning the generation and exchange of the session key `Kab`. The messages `5-7` are the mutual authentification, this second part of the protocol can be repeated alone several times, until the ticket `{A, Kab, Tb}Kbs` expires (it is called *repeated authentication*).

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` in that session.

The protocol must also ensures mutual authentication of `A` and `B`.

References

[NS93]

Claimed attacks

1. From [HLL+95], see also BAN simplified version of Yahalom for the first 4 messages, where `B` accepts the nonce `Na` has the fresh shared key `Kab`.

1.	I(A)	->	B	:	A, Na
2.	B	->	I(S)	:	B, {A, Na, Tb}Kbs, Nb
3.					omitted
4.	I(A)	->	B	:	{A, Na, Tb}Kbs, {Nb}Na
5.	I(A)	->	B	:	Ma, {A, Na, Tb}Kbs
6.	B	->	I(A)	:	Mb, {Ma}Na
7.	I(A)	->	B	:	{Mb}Na

See Hwang modified version of Neumann Stubblebine for a modified version preventing this attack.

2. From [HLL+95]. This attack concerns the repeated authentication part, assuming `Kab` has been recorded in a previous legitimate run of the protocol.

i.5.	I(A)	->	B	:	Ma, { A, Kab, Tb }Kbs
i.6.	B	->	I(A)	:	Mb, {Ma}Kab
ii.5.	I(A)	->	B	:	Mb, {A, Kab, Tb}Kbs
ii.6.	B	->	I(A)	:	Mb', {Mb}Kab
i.7.	I(A)	->	B	:	{Mb}Kab

3. From [Wei99]. In this attack, the intruder `I` can get as many ciphers `{A, Kiab, Tb}Kbs` as needed to start a known plaintext attack in order to break `Kbs`.

a.2.	I(B)	->	S	:	B, {A, K0ab, Tb}Kbs, Nb
a.3.	S	->	I(A)	:	{B, Na, K1ab, Tb}Kas, {A, K1ab, Tb}Kbs, Nb
b.2.	I(B)	->	S	:	B, {A, K1ab, Tb}Kbs, Nb
b.3.	S	->	I(A)	:	{B, Na, K2ab, Tb}Kas, {A, K2ab, Tb}Kbs, Nb
					etc

See also

Yahalom

Citations

[HLL+95] Tzonelih Hwang, Narn-Yoh Lee, Chuang-Ming Li, Ming-Yung Ko, and Yung-Hsiang Chen. Two attacks on neumann-stubblebine authentication protocols. *Information Processing Letters*, 53:103 – 107, 1995.

[NS93] B. Clifford Neumann and Stuart G. Stubblebine. A note on the use of timestamps as nonces. *Operating Systems Review*, 27(2):10–14, april 1993.

[Wei99] Christoph Weidenbach. Towards an automatic analysis of security protocols. In Harald Ganzinger, editor, *Proceedings of the 16th International Conference on Automated Deduction*, volume 1632 of *LNAI*, pages 378–382. Springer, 1999.