Hwang modified version of Neumann Stubblebine

Author(s): T. Hwang and N.Y. Lee and C.M. Li and M.Y. Ko and Y.H. Chen 1995

Last modified November 11, 2002

Summary: Modified version of the Neumann Stubblebine protocol, to correct attack of the repeated authentification part.

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, Nb}Kbs
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, {Mb}Kab
7.    A  ->  B   :    {Mb}Kab
```

Description of the protocol rules

See Neumann Stubblebine. The messages 1-4 are the part concerning the generation and exchange of the session key Kab. The messages 5-7 is the *repeated authentication* part.

Requirements

See Neumann Stubblebine.

References

[HLL$^+$95]

Claimed attacks

In [CJ95], Clark and Jacob describe an attack depending on the encryption method (when cipher block chaining is performed for encryption).

See also

Neumann Stubblebine

Citations

[CJ95] John A Clark and Jeremy L Jacob. On the security of recent protocols. *Information processing Letters*, 56:151–155, 1995.

[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.