Denning-Sacco shared key

Author(s): Dorothy E. Denning and Giovanni Maria Sacco 1981

Last modified November 12, 2002

Summary: Modified version of the Needham Schroeder Symmetric Key with timestamps to fix the freshness flaw. Distribution of a shared symmetric key by a trusted server and mutual authentification. Symmetric key cryptography with server and timestamps.

Protocol specification (in common syntax)

```
A, B, S :          principal
Kas, Kbs, Kab :    key
T :                timestamp

1.    A   ->  S   :    A, B
2.    S   ->  A   :    {B, Kab, T, {Kab, A, T}Kbs}Kas
3.    A   ->  B   :    {Kab,A, T}Kbs
```

Description of the protocol rules

The nonces of Needham Schroeder Symmetric Key (for mutual authentication of A and B) have been replaced by a timestamp T.

The shared symmetric key established by the protocol is Kab.

Requirements

See Needham Schroeder Symmetric Key.

References

[DS81]

Claimed attacks

This protocol is subject to a mutiplicity attack [Low97].

```
i.1.       A     ->  S   :    A, B
i.2.       S     ->  A   :    {B, Kab, T, {Kab, A, T}Kbs}Kas
i.3.       A     ->  B   :    {Kab,A, T}Kbs
ii.3.    I(A)    ->  B   :    {Kab,A, T}Kbs
```

In session ii, B thinks that A wants to establish a new shared key and accepts it.

See also

Lowe modified Denning-Sacco shared key, Needham Schroeder Symmetric Key.

Citations

[DS81] D. Denning and G. Sacco. Timestamps in key distributed protocols. *Communication of the ACM*, 24(8):533–535, 1981.

[Low97] Gavin Lowe. A family of attacks upon authentication protocols. Technical Report 1997/5, Department of Mathematics and Computer Science, University of Leicester, 1997.