Kao Chow Authentication v.2

Author(s): I Long Kao and Randy Chow 1995
Last modified November 11, 2002

Summary: Key distribution and authentication protocol. Symmetric keys cryptography with server.

Remark

This protocol is a correction of Kao Chow Authentication v.1 to prevent a freshness attack à la Denning Sacco attack (see Needham Schroeder Symmetric Key).

Protocol specification (in common syntax)

```
A, B, S :          principal
Na, Nb :           number
Kab, Kbs, Kas :    key

1.    A  ->  S   :    A, B, Na
2.    S  ->  B   :    {A, B, Na, Kab, Kt}Kas, {A, B, Na, Kab, Kt}Kbs
3.    B  ->  A   :    B, {A, B, Na, Kab, Kt}Kas, {Na, Kab}Kt, Nb
4.    A  ->  B   :    {Nb, Kab}Kt
```

Description of the protocol rules

See Kao Chow Authentication v.1. `Kt` is an additional fresh symmetric key whose purpose is to prevent a freshness attack as in Kao Chow Authentication v.1.

Requirements

See Kao Chow Authentication v.1.

References

[KC95].

This specification of the protocol differs from the one in [CJ97].

Claimed proofs

[KC95]

See also

Kao Chow Authentication v.1, Kao Chow Authentication v.3, Needham Schroeder Symmetric Key, Neumann Stubblebine.

Citations

[CJ97] John Clark and Jeremy Jacob. A survey of authentication protocol literature : Version 1.0., November 1997.

[KC95] I Lung Kao and Randy Chow. An efficient and secure authentication protocol using uncertified keys. *Operating Systems Review*, 29(3):14–21, 1995.