Kao Chow Authentication v.3

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 an extension of Kao Chow Authentication v.2 to encompass tickets.

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   :    {A, B, Na, Kab, Kt}Kas, {Na, Kab}Kt, Nb, {A, B, Ta, Kab}Kbs
4.    A  ->  B   :    {Nb, Kab}Kt, {A, B, Ta, Kab}Kbs
```

Description of the protocol rules

In message `3`, `B` generates a new ticket `{A, B, Ta, Kab}Kbs` containing `Kab` and a timestamp `Ta`.

Requirements

See Kao Chow Authentication v.1.

References

[KC95].

See also

Kao Chow Authentication v.1, Kao Chow Authentication v.2, Needham

Schroeder Symmetric Key, Neumann Stubblebine.

Citations

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