Kao Chow Authentication v.1

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.

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

Description of the protocol rules

`Kas` and `Kbs` are symmetric keys whose values are initially known only by `A` and `S`, respectively `B` and `S`.

`Na` and `Nb` are nonces for mutual authentication and to verify the authenticity of the fresh symmetric key `Kab`.

The messages `3` and `4` are *repeated authentication*: after that messages `1` and `2` have completed successfully, `3` and `4` can be played several times by `B` before starting a secrete communication with `A` encrypted with the session key `kab` (see also Neumann Stubblebine for repeated authentication).

Remark

This protocol has been designed to prevent the freshness attack on the repeated authentication part of the Neumann Stubblebine protocol. Indeed, the nonce `Na` in the ciphers of message `2` prevent a shared key compromised after another run of the protocol to be reused.

However, as shown below, an attack of this kind is still possible. This flaw is fixed in Kao Chow Authentication v.2.

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.

When A, resp. B, receives the key Kab in message 3, resp. 2, this key must have been issued in the same session by the server S with whom A has started to communicate in message 1.

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

References

[KC95]. The protocol is presented as specified in [CJ97].

Claimed attacks

As described in [KC95], this protocol suffers the same kind of attack as the Denning Sacco freshness attack on Needham Schroeder Symmetric Key, when an older session symmetric key Kab has been compromised.

```
i.1.       A    ->    S     :    A, B, Na
i.2.       S    ->    B     :    {A, B, Na, Kab}Kas, {A, B, Na, Kab}Kbs
                                 assume that Kab is compromised
ii.1.                            Omitted
ii.2.    I(S)   ->    B     :    {A, B, Na, Kab}Kas, {A, B, Na, Kab}Kbs
ii.3.      B    ->  I(A)    :    {A, B, Na, Kab}Kas, {Na}Kab, N'b
ii.4.    I(A)   ->    B     :    {N'b}Kab
```

See also

Kao Chow Authentication v.2, 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.