Otway Rees

Author(s): D. Otway and O. Rees January 1997

Last modified November 12, 2002

Summary: Distribution of a shared symmetric key by a trusted server. Symmetric key cryptography with server.

Protocol specification (in common syntax)

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

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

Description of the protocol rules

The nonce M identifies the session number.

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

Kab is a fresh symmetric key generated by S in message 3 and distributed to B, directly in message 3, and to A, indirectly, when B forwards blindly {Na, Kab}Kas to A in message 4.

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 B has started to communicate in message 2.

References

[OR87]

Claimed attacks

Type flaw in [CJ97], where `A` will accept in last message 4 the triple `(M, A, B)` as a fresh key `Kab`.

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

Citations

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

[OR87] D. Otway and O. Rees. Efficient and timely mutual authentication. *Operating Systems Review*, 21(1):8–10, 1987.