Woo and Lam Pi f

Author(s): Woo, Lam 1994
Last modified October 27, 2001

Summary: One way authentification protocol with public keys and trusted server.

Protocol specification (in common syntax)

```
A, B, S :  principal
shared :   (principal, principal):key
Nb :       nonce

1..    A  ->  B   :    A
2..    B  ->  A   :    Nb
3..    A  ->  B   :    {A,B,Nb}shared(A, S)
4..    B  ->  S   :    {A, B, Nb, {A, B, Nb}shared(A, S)}shared(B, S)
5..    S  ->  B   :    {A, B, Nb}shared(B, S)
```

Description of the protocol rules

`shared(A, S)` is a long term symmetric key shared by `A` and `S`. Initially, `A` only knowns `shared(A, S)` and the name of `B`, `B` only knowns `shared(B, S)` and `S` knowns all shared keys, i.e. `S` given any principal's name `X`, `S` knowns `shared(X, S)`, or in other terms, `S` knows the "function" `shared`.

Requirements

Woo and Lam give in [WL94] the following definition of correctness for this protocol:

whenever the principal `B` finishes the execution of the protocol, the initiator of the protocol execution is in fact the principal `A` claimed in message `1`.

References

[WL94], [CJ97].

Claimed proofs

[WL94]

Claimed attacks

No known attacks.

See also

Woo and Lam Pi 1, Woo and Lam Pi 2, Woo and Lam Pi 3, Woo and Lam Pi.

Citations

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

[WL94] T. Y. C. Woo and S. S. Lam. A lesson on authentication protocol design. *Operating Systems Review*, 1994.