Woo and Lam Mutual Authentication

Author(s): T.Y.C Woo and S.S. Lam 1994
Last modified November 10, 2002

Summary: Key distribution and mutual authentication with trusted server and symmetric keys.

Protocol specification (in common syntax)

```
P, Q, S :        principal
Kps, Kqs, Kpq :  key
N1, N2 :         number

1.    P  ->  Q  :    P, N1
2.    Q  ->  P  :    Q, N2
3.    P  ->  Q  :    {P, Q, N1, N2}Kps
4.    Q  ->  S  :    {P, Q, N1, N2}Kps, {P, Q, N1, N2}Kqs
5.    S  ->  Q  :    {Q, N1, N2, Kpq}Kps, {P, N1, N2,Kpq}Kqs
6.    Q  ->  P  :    {Q, N1, N2, Kpq}Kps, {N1, N2}Kpq
7.    P  ->  Q  :    {N2}Kpq
```

Description of the protocol rules

`Kpq` is a fresh symmetric key created at message `5` by the server `S`.

`N1` and `N2` are nonces.

`Kps` and `Kqs` are symmetric keys whose values are initially known only by `P` and `S`, respectively `P` and `S`.

Requirements

The protocol must guaranty the secrecy of `Kpq`: in every session, the value of `Kpq` must be known only by the participants playing the roles of `P`, `Q` and `S`.

The protocol must also ensures mutual authentication of `P` and `Q`.

References

[WL94]

Claimed attacks

1. Parallel session replay attack, [CJ], and [CJ97]. In this attack, the intruder `I` initiates a session `ii` in order to make `P` accept a non-fresh key.

```
i.1.      P    ->    I    :    P, N1
ii.1.     I    ->    P    :    I, N1
ii.2.     P    ->    I    :    P, N2
i.2.      I    ->    P    :    I, N2
i.3.      P    ->    I    :    {P, I, N1, N2}Kps
i.4.      I    ->    S    :    {P, I, N1, N2}Kps, {P, I, N1, N2}Kis
i.5.      S    ->    I    :    {I, N1, N2, Kpi}Kps, {P, N1, N2, Kpi}Kis
i.6.      I    ->    P    :    {I, N1, N2, Kpi}Kps, {N1, N2}Kpi
i.7.      P    ->    I    :    {N2}Kpi
ii.3.     I    ->    P    :    {I, P, N1, N2}Kis
ii.4.     P    ->  I(S)   :    {I, P, N1, N2}Kis, {I, P, N1, N2}Kps
ii.5.   I(S)   ->    P    :    {I, N1, N2, Kpi}Kis, {I, N1, N2, Kpi}Kps
ii.6.     P    ->    I    :    {P, N1, N2, Kpi}Kis, {N1, N2}Kpi
ii.7.     I    ->    P    :    {N2}Kpi
```

2. [Low96]. `bit-string` represent an arbitrary number.

```
i.1.    I(P)   ->    Q    :    P, Q
i.2.      Q    ->  I(P)   :    Q, N2
i.3.    I(P)   ->    Q    :    bit-string
i.4.      Q    ->  I(S)   :    bit-string, {P, Q, Q, N2}Kps
ii.1.   I(P)   ->    Q    :    P, N2
ii.2.     Q    ->  I(P)   :    Q, N3
ii.3.   I(P)   ->    Q    :    bit-string'
ii.4.     Q    ->  I(S)   :    bit-string', {P, Q, N2, N3}Kps
i.5.    I(S)   ->    Q    :    bit-string'', {P, Q, N2, N3}Kps
i.6.      Q    ->  I(P)   :    bit-string'', {Q, N2}N3
i.7.    I(P)   ->    Q    :    {N2}N3
```

Citations

[CJ] John Clark and Jeremy Jacob. Freshness is not enough : Note on trusted nonce generation and malicious principals. attack on a mutual authentification protocol by Woo and Lam.

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

[Low96] Gavin Lowe. Some new attacks upon security protocols. In IEEE Computer Society Press, editor, *In Proceedings of the Computer Security Foundations Workshop VIII*, 1996.

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