Lowe modified KSL

Author(s): Gavin Lowe 1996
Last modified December 2, 2002

Summary: Lowe modified version of the KSL protocol to prevent authentication attacks. Distribution of a session key and a ticket and repeated mutual authentication. Symmetric key cryptography with server.

Protocol specification (in common syntax)

```
A, B, S :               principal
Na, Nb, Nc, Ma, Mb :    number
Kas, Kbs, Kab, Kbb :    key
Tb :                    generalizedTimestamp

1.    A  ->  B  :    Na, A
2.    B  ->  S  :    Na, A, Nb, B
3.    S  ->  B  :    {A, Nb Kab}Kbs, {Na, B, Kab}Kas
4.    B  ->  A  :    {Na, B, Kab}Kas, {Tb, A, Kab}Kbb, Nc, {B, Na}Kab
5.    A  ->  B  :    {Nc}Kab

6.    A  ->  B  :    Ma, {Tb, A, Kab}Kbb
7.    B  ->  A  :    Mb, {Ma, B}Kab
8.    A  ->  B  :    {A, Mb}Kab
```

Description of the protocol rules

See KSL.

The version given above has been devised from the following modifications to KSL advised in [Low96]:

- “change the message 3 so that the two encrypted components have different forms” (in order to break symmetry),
- “make the encrypted components in 4, 7 and 8 different”,
- “include either A’s or B’s identity in these last three components”.

Requirements

See KSL.

References

[Low96]

See also

KSL

Citations

[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.