BAN modified version of CCITT X.509 (3)

Author(s): Michael Burrows and Martin Abadi and Roger Needham 1989
Last modified January 16, 2003

Summary: Modified version of the three messages protocol in the recommendations of the CCITT for the CCITT.X.509 standard (CCITT X.509 (3)).

Protocol specification (in common syntax)

```
A, B :    principal
Na, Nb :  nonce
Ya, Yb :  userdata
Xa, Xb :  userdata
PK, SK :  principal -> key (keypair)

1.   A  ->  B  :   A, {Na, B, Xa, {Ya}PK(B)}SK(A)
2.   B  ->  A  :   B, {Nb, A, Na, Xb, {Yb}PK(A)}SK(B)
3.   A  ->  B  :   A, {B, Nb}SK(A)
```

Description of the protocol rules

Compared to CCITT X.509 (3), the identity of B has been added to the signature in message 3. This prevents the [BAN89] attack on the CCITT X.509 (3) protocol, which can occur when B does not check the timestamps. With this modification, the timestamps become redundant and can be removed.

Requirements

See CCITT X.509 (3).

References

[BAN89].

See also

CCITT X.509 (1), CCITT X.509 (1c), CCITT X.509 (3).

Citations

[BAN89] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. Technical Report 39, Digital Systems Research Center, february 1989.