CCITT X.509 (3)

Author(s): CCITT 1987
Last modified November 22, 2002

Summary: Three messages protocol in the recommendations of the CCITT for the CCITT.X.509 standard.

Remark

This protocol presented here is actually a simplified version from [BAN89] and [AN96].

Protocol specification (in common syntax)

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

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

Description of the protocol rules

See CCITT X.509 (1).

Remark

As in the case of CCITT X.509 (1), in the original protocol specification [CCI87], only a hash of the data is signed, for efficiency reasons. Hence the messages specification ought to be:

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

where `h` is a one-way function.

Requirements

The protocol must ensure the confidentiality of `Ya` and `Yb`: if `A` and `B` follow the protocol, then an attacker should not be able to obtain `Ya` or `Yb`.

The protocol must ensure the recipient `B` of the message `1` that the data `Xa` and `Ya` originate from `A`.

The protocol must ensure the recipient `A` of the message `2` that the data `Xb` and `Yb` originate from `B`.

References

[BAN89], [CCI87].

Claimed attacks

1. This parallel session attack presented in [BAN89] works if `B` does not check the timestamp `Ta` in the first message.

```
i.1.      A    ->  I(B)   :    A, {Ta, Na, B, Xa, {Ya}PK(B)}SK(A)
i.1.    I(A)   ->   B     :    A, {Ta, Na, B, Xa, {Ya}PK(B)}SK(A)
i.2.      B    ->  I(A)   :    B, {Tb, Nb, A, Na, Xb, {Yb}PK(A)}SK(B)
ii.1.     A    ->   I     :    A, {Ta', Na', C, Xa', {Ya'}PK(I)}SK(A)
ii.2.     I    ->   A     :    I, {Ti, Nb, A, N'a,Xi, {Yi}PK(A)}SK(I)
ii.3.     A    ->   I     :    A, {Nb}SK(A)
ii.3.   I(A)   ->   B     :    A, {Nb}SK(A)
```

2. Another attack can be found in [lM90].

See also

CCITT X.509 (1), CCITT X.509 (1c), BAN modified version of CCITT X.509 (3).

Citations

[AN96] Martín Abadi and Roger Needham. Prudent engineering practice for cryptographic protocols. *IEEE Transactions on Software Engineering*, 22(1):6–15, January 1996.

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

[CCI87] CCITT. The directory authentification framework. Draft Recommendation X.509, 1987. Version 7.

[lM90] Colin l'Anson and Chris Mitchell. Security defects in the ccitt recomendation x.509 - the directory authentication framework. *Computer Communication Review*, 20(2):30–34, april 1990.