Clark and Jacob modified Hwang and Chen modified SPLICE/AS

Author(s): 1995
Last modified November 11, 2002

Summary: This modified version corrects a flaws in Hwang and Chen modified SPLICE/AS. Mutual authentication protocol with public key cryptography with a certification authority signing and distributing public keys.

Protocol specification (in common syntax)

```
S, C, AS :    principal
N1, N2, N3 :  nonce
T :           timestamp
L :           lifetime
pk, sk :      principal -> key (keypair)
```

```
1.    C   ->  AS   :    C, S, N1
2.    AS  ->  C    :    AS, {AS, C, N1, S, pk(S)}sk(AS)
3.    C   ->  S    :    C, S, {T, L, {C, N2}pk(S)}sk(C)
4.    S   ->  AS   :    S, C, N3
5.    AS  ->  S    :    AS, {AS, S, N3, C, pk(C)}sk(AS)
6.    S   ->  C    :    S, C, {inc(N2)}pk(C)
```

Remark

This protocol is an optimised version of the following modification of Hwang and Chen modified SPLICE/AS:

```
1.    C   ->  AS   :    C, S, N1
2.    AS  ->  C    :    AS, {AS, C, N1, S, pk(S)}sk(AS)
3.    C   ->  S    :    C, S, {C, T, L, {C, N2}pk(S)}sk(C)
4.    S   ->  AS   :    S, C, N3
5.    AS  ->  S    :    AS, {AS, S, N3, C, pk(C)}sk(AS)
6.    S   ->  C    :    S, C, {S, inc(N2)}pk(C)
```

The messages `3` and `6` are optimised by suppressing some redundancies: the redundant `C` is not included in the signed part of message `3` and `S` in not included in the cipher of message `6`

Description of the protocol rules

See SPLICE/AS. The difference with Hwang and Chen modified SPLICE/AS

is in messages Note that the name of the owner of the public key is included in certificate to overcomes the flaws of SPLICE/AS presented in [HC95] (i.e. a certificate for the public key `pk(S)` is here `{AS, C, N1, S, pk(S)}sk(AS)` rather than `{AS, C, N1, pk(S)}sk(AS)` in SPLICE/AS).

Requirements

See SPLICE/AS.

References

[CJ95].

Claimed attacks

Lowe [Low97] demonstrate a multiplicity attack on this protocol, where `I` impersonates `C` in a new session `ii`, by replaying message `3` of session `i`. `I` does however not learn `N2`.

```
i.1.      C    ->   AS    :    C, S, N1
i.2.     AS    ->    C    :    AS, {AS, C, N1, S, pk(S)}sk(AS)
i.3.      C    ->    S    :    C, S, {T, L, {C, N2}pk(S)}sk(C)
i.4.      S    ->   AS    :    S, C, N3
i.5.     AS    ->    S    :    AS, {AS, S, N3, C, pk(C)}sk(AS)
i.6.      S    ->    C    :    S, C, {inc(N2)}pk(C)
ii.3.  I(C)    ->    S    :    C, S, {T, L, {C, N2}pk(S)}sk(C)
ii.4.     S    ->   AS    :    S, C, N'3
ii.5.    AS    ->    S    :    AS, {AS, S, N'3, C, pk(C)}sk(AS)
ii.6.     S    ->  I(C)   :    S, C, {inc(N2)}pk(C)
```

Lowe suggests in [Low97] to add a nonce challenge to prevent this attack.

See also

SPLICE/AS, Hwang and Chen modified SPLICE/AS.

Citations

[CJ95] John A Clark and Jeremy L Jacob. On the security of recent protocols. *Information processing Letters*, 56:151–155, 1995.

[HC95] Tzonelih Hwang and Yung-Hsiang Chen. On the security of splice/as : The authentication system in wide internet. *Information Processing Letters*, 53:97–101, 1995.

[Low97] Gavin Lowe. A family of attacks upon authentication protocols. Technical Report 1997/5, Department of Mathematics and Computer Science, University of Leicester, 1997.