Hwang and Chen modified SPLICE/AS

Author(s): Tzonelih Hwang and Yung-Hsiang Chen 1995
Last modified November 11, 2002

Summary: This modified version correct two flaws in 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, {C, T, L, {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)
```

Description of the protocol rules

See SPLICE/AS. 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

[HC95].

Claimed attacks

[CJ95]. Only the messages 3 and 6 are relevant in this attack, in which the intruder I learn the secret N2. This attack concerns both the secrecy of N2 and its authenticity.

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

See also

SPLICE/AS, Clark and Jacob modified 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.