**SPLICE/AS**

**Author(s):** Suguru Yamaguchi, Kiyohiko Okayama, and Hideo Miyahara
November 1991
*Last modified November 26, 2002*

**Summary:** Mutual authentication protocol. 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, pk(S)}sk(AS)
3. C -> S : C, S, {C, T, L, {N2}pk(S)}sk(C)
5. AS -> S : AS, {AS, S, N3, pk(C)}sk(AS)
6. S -> C : S, C, {S, inc(N2)}pk(C)
```

**Description of the protocol rules**

`key` is the type of public/private keys. The functions `pk` and `sk` associate to a principal’s name its public key, resp. private key.

We assume that initially, the client `C` and the server `S` only know their own public and private key, and that the authority `AS` known the function `pk`, i.e. he knows everyone’s public key.

{AS, C, N1, pk(S)}sk(AS) (in message 2) and {AS, S, N3, pk(C)}sk(AS) (in message 5) are certificates signed and distributed by the authority `AS`, for the respective public keys `pk(S)` and `pk(C)`.

After a successful run of the protocol, the value of `N2` can be used by `C` and `S` as a symmetric key for secure communications.

**Requirements**

The protocol must guaranty the secrecy of `N2`: in every session, the value of `N2` must be known only by the participants playing the roles of `C, S`.

[http://www.lsv.ens-cachan.fr/spore](http://www.lsv.ens-cachan.fr/spore)
The protocol must also ensure C that S has received N2 and S that the N2 he has received in message 3 originated from C.

References

[YOM91]

Claimed attacks

1. In an attack described in [HC95], the intruder I can impersonate the client C and obtain N2 in a single session (i.e. without even running a parallel session).

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

   In message 5, the server S accepts the certificate {AS, S, N3, pk(I)}sk(AS) from AS as a certificate of the public key of C (note that the certificates do not contain the name of the owner of public key) and hence crypts the data in the last message 6 with the public key of I.

2. In this second (symmetric) attack from [HC95], the intruder I can impersonate the server S and obtain N2.

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

3. Lowe outlined (see [CJ97]) that a malicious C can replay the message 3 (the first message concerning S) several times, with new values of T and L, to restart authentication with an old value of N2.
See also

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

Citations

