SK3

Author(s): Victor Shoup and Avi D. Rubin 1996
Last modified February 11, 2003

Summary: Symmetric key distribution using Smart Cards, by Shoup and Rubin.

Protocol specification (in common syntax)

`A, B, S, Ca, Cb` :	`principal`
`Ka, Kb` :	`symkey`
`Kac, Kbc` :	`symkey`
`Na, Nb` :	`nonce`
`0,1,2` :	`number`

alias Kab = {`A, 0`}`Kb`
alias Pab = Kab + {`B, 1`}`Ka`

```
1.   A  -> S  : A, B
2.   S  -> A  : Pab, {Pab, B, 2}Ka
3.   A  -> Ca : A
4.   Ca -> A  : Na, {Na, 1, 1}Kac
5.   A  -> B  : A, Na
6.   B  -> Cb : A, Na
7.   Cb -> B  : Nb, {Nb, 0, 0}Kab, {Na, Nb, 1}Kab, {Nb, 0, 1}Kab
8.   B  -> A  : Nb, {Na, Nb, 1}Kab
9.   A  -> Ca : B, Na, Nb, Pab, {Pab, B, 2}Ka, {Na, Nb, 1}Kab, {Nb, 0, 1}Kab
10.  Ca -> A  : {Nb, 0, 0}Kab, {Nb, 0, 1}Kab
11.  A  -> B  : {Nb, 0, 1}Kab
```

Description of the protocol rules

- the operator {`M`}`K` denotes DES encryption.
- the operator `+` is xor.
- the principal `Ca` (resp. `Cb` is a smart card connected to `A` (resp. `B`) and used to store its long term keys.
- **NB:** the connection between `A` and `Ca` (resp. `B` and `Cb`) is assumed to be secure (i.e. no intruder has the capability to listen to this connection).

- Ka (resp. Kb) is a long term (symmetric) keys associated to the principal A (resp. B). It is assumed to be known initially only by Ca (resp. Cb) and the server S.
- Kac (resp. Kbc) is a secret symmetric key share (and initially only known by) A and Ca (resp. B and Cb).
- 0, 1, 2 are arbitrary padding constants, known to every principal.

1,2 A requires and obtains from the server S the pair key Pab associed to A and B. {Pab, B, 2}Ka is a verifier for this value.

3,4 A requires and abtains a nonce Na from her smart card Ca. {Na, 1, 1}Kac is a verifier. In [SR96], it is suggested to use a 8 bytes counter on Ca to generate Na.

5 A sends the nonce, meaning she request the establishment of a session symmetric key.

6,7 B obtains the nonce Nb from Cb (same remark as in 3,4 for the counters). {Nb, 0, 0}Kb is a session key and {Na, Nb, 1}Kab, and {Nb, 0, 1}Kab are verifiers respectively for A and B.

8 B transmits the nonce Nb and A's verifier to A.

9 the nonce Nb and A's verifier are transmitted to A.

10 A's smart card Ca makes the verifications, computes the session key {Nb, 0, 0}Kb and transmits it to A.

11 A aknowledge to B, who can compare this message to his verifier remaining from message 7.

Requirements

The session key {Nb, 0, 0}Kb must remain secret.

References

[SR96]. Some variants and implementation issues are discussed in the update [Sho96]. See also the implementor's paper [JHC+98].

Claimed proofs

The proof of [SR96] is based on the probabilistic definition of secure key distribution from Bellare and Rogaway [BR95].

[Bel01] uses a theorem proving approach, following Paulson's inductive method.

Remark

See [Sho96]. The nonce `Na` that `A` obtains from his smart card `Ca` must actually be truly random and not implemented by counters as first suggested in [SR96].

Indeed, if the next value of `Na` (sent in message `5` of session `i`) is predictable (let us call it `Na'`), then then the intruder `I` can query `B` for the verifiers including `Na'` (session `ii`) and use them to answer the next challenge of `A` (hence, authentication error in session `iii`).

```
 i.5.        A    ->    B    :    A, Na
 ii.5.     I(A)   ->    B    :    A, Na'
 ii.6.       B    ->    Cb   :    A, Na'
 ii.7.       Cb   ->    B    :    Nb', {Nb', 0, 0}Kab, {Na', Nb', 1}Kab, {Nb', 0, 1}Kab
 ii.8.       B    ->    A    :    Nb', {Na', Nb', 1}Kab
 iii.5.      A    ->   I(B)  :    A, Na'
 iii.8.    I(B)   ->    A    :    Nb', {Na', Nb', 1}Kab
```

According to [Sho96], the nonce `Nb` may though be a counter.

Citations

[Bel01] Giampaolo Bella. Mechanising a protocol for smart cards. In *Proc. of e-Smart 2001, international conference on research in smart cards*, LNCS. Springer-Verlag, september 2001.

[BR95] Mihir Bellare and Phillip Rogaway. Provably secure session key distribution– the three party case. In *Proceedings 27th Annual Symposium on the Theory of Computing*, ACM, pages 57–66, 1995.

[JHC+98] Rob Jerdonek, Peter Honeyman, Kevin Coffman, Kim Rees, and Kip Wheeler. Implementation of a provably secure, smartcard-based key distribution protocol. In *In Proceedings of the Third Smart Card Research and Advanced Application Conference*, 1998.

[Sho96] Victor Shoup. A note on session key distribution using smart cards. http://www.shoup.net/papers/update.ps, july 1996.

[SR96] Victor Shoup and Avi Rubin. Session key distribution using smart cards. In *In Proceedings of Advances in Cryptology, EUROCRYPT'96*, volume 1070 of *LNCS*. Springer-Verlag, 1996.