three-pass mutual authentication

Protocol Purpose

Two parties authenticate each other. Aim of the Mutual authentication is to make sure to each of the parties of the other's identity. In this protocol a confirmation of the successful authentication is sent by the initiator.

Definition Reference

- [CJ, ISO97]

Model Authors

- Haykal Tej, Siemens CT IC 3, 2003 and
- Luca Compagna et al, AI-Lab DIST University of Genova, November 2004

Alice&Bob style

```
1. B -> A : Nb, Text1
2. A -> B : PKa,A,{PKa,A}inv(PKs),Na,Nb,B,Text3,{Na,Nb,B,Text2}inv(PKa)
3. B -> A : PKb,B,{PKb,B}inv(PKs),Nb,Na,A,Text5,{Nb,Na,A,Text4}inv(PKb)
```

Problems considered: 2

Attacks Found

None

Further Notes

`inv(PKs)` is the private key of the server `C`; `{PKa,A}inv(PKs)` is the certificate of agent `A`, and `{PKb,B}inv(PKs)` is the certificate of agent `B`.

HLPSL Specification

```
role iso4_Init ( A,B: agent,
                 Pkb,Pks: public_key,
                 Snd,Rec: channel(dy))
played_by B
def=

  local  State         : nat,
         Pka           : public_key,
         Nb            : text,
         Na,Text2,Text3: text

  const ctext1,ctext4,ctext5: text

  init State := 0

  transition

   1. State = 0
      /\ Rec(start)
      =|>
      State' := 1
      /\ Nb' := new()
      /\ Snd(Nb'.ctext1)
      /\ witness(B,A,nb,Nb')

   2. State = 1
      /\ Rec(Pka'.A.{Pka'.A}_inv(Pks).Na'.Nb.B.Text3'.
             {Na'.Nb.B.Text2'}_inv(Pka'))
      =|>
      State' := 2
      /\ Snd(Pkb.B.{Pkb.B}_inv(Pks).Nb.Na'.A.ctext5.{Nb.Na'.A.ctext4}_inv(Pkb))
      /\ request(B,A,na,Na')

end role
```

```
role iso4_Resp ( B,A: agent,
                 Pka,Pks: public_key,
                 Snd,Rec: channel(dy))
played_by A
def=

  local  State               : nat,
         Pkb                 : public_key,
         Na                  : text,
         Nb,Text1,Text4,Text5: text

  const ctext2,ctext3: text

  init State := 0

  transition

   1. State = 0
      /\ Rec(Nb'.Text1')
      =|>
      State' := 1
      /\ Na' := new()
      /\ Snd(Pka.A.{Pka.A}_inv(Pks).
             Na'.Nb'.B.ctext3.{Na'.Nb'.B.ctext2}_inv(Pka))
      /\ witness(A,B,na,Na')

   2. State = 1
      /\ Rec(Pkb'.B.{Pkb'.B}_inv(Pks).
             Nb.Na.A.Text5'.{Nb.Na.A.Text4'}_inv(Pkb'))
      =|>
      State' := 2
      /\ request(A,B,nb,Nb)

end role
```

```
role session (A,B:agent,
```

```
              Pka,Pkb,Pks: public_key) def=

  local SA,RA,SB,RB: channel (dy)

  composition

          iso4_Init(A,B,Pkb,Pks,SA,RA)
       /\ iso4_Resp(B,A,Pka,Pks,SB,RB)

end role
```

```
role environment() def=

 const na, nb             : protocol_id,
       a, b, i            : agent,
       pka, pkb, pks, pki : public_key

 intruder_knowledge={a,b,pki,inv(pki),pks,
                     ctext1,ctext4,ctext5,{pki.i}_inv(pks),
                     ctext2,ctext3,{pki.i}_inv(pks)}

 composition

        session(a,b,pka,pkb,pks)
     /\ session(a,i,pka,pki,pks)
     /\ session(i,b,pki,pkb,pks)

end role
```

```
goal

   %ISO4_Resp authenticates ISO4_Init on nb
   authentication_on nb

   %ISO4_Init authenticates ISO4_Resp on na
   authentication_on na
```

```
end goal
```

```
environment()
```

References

[CJ] J. Clark and J. Jacob. A Survey of Authentication Protocol Literature: Version 1.0, 17. Nov. 1997. URL: www.cs.york.ac.uk/~jac/papers/drareview.ps.gz.

[ISO97] ISO/IEC. ISO/IEC 9798-3: Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques, 1997.