two-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 authentication should be achieved by a single encrypted message sent from each party.

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

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

Problems considered: 2

Attacks Found

The intruder can attack this protocol by simple eavesdropping and replaying the messages.

```
i     -> (a,6) : start
(a,6) -> i     : pka,a,{pka,a}inv(pks),na(a,6),b,ctext2,
                 {na(a,6),b,ctext1}inv(pka)
i     -> (b,9) : start
(b,9) -> i     : pkb,b,{pkb,b}inv(pks),na(b,9),a,ctext2,
                 {na(b,9),a,ctext1}inv(pkb)
i     -> (a,6) : pkb,b,{pkb,b}inv(pks),na(b,9),a,ctext2,
                 {na(b,9),a,ctext1}inv(pkb)
```

Further Notes

HLPSL Specification

```
role iso3_Init( A, B     : agent,
                Pka, Pks : public_key,
                Snd, Rcv : channel(dy))
played_by A
def=

  local  State             : nat,
         Na                : text,
         Nb, Text3, Text4  : text,
         Pkb               : public_key

  init State := 0

  transition

   1. State = 0
      /\ Rcv(start)
      =|>
      State' := 1
      /\ Na' := new()
      /\ Snd(Pka.A.{Pka.A}_inv(Pks).Na'.B.ctext2.{Na'.B.ctext1}_inv(Pka))
      /\ witness(A,B,na,Na')
   2. State = 1
      /\ Rcv(Pkb'.B.{Pkb'.B}_inv(Pks).Nb'.A.Text4'.{Nb'.A.Text3'}_inv(Pkb'))
      =|>
      State' := 2
      /\ wrequest(A,B,nb,Nb')

end role
```

```
role iso3_Resp (B, A     : agent,
                Pkb, Pks : public_key,
                Snd, Rcv : channel(dy))
played_by B
def=

   local  State          : nat,
          Nb             : text,
          Na,Text1,Text2 : text,
          Pka            : public_key

   init State := 0

   transition

   1. State = 0
      /\ Rcv(Pka'.A.{Pka'.A}_inv(Pks).Na'.B.Text2'.{Na'.B.Text1'}_inv(Pka'))
      =|>
      State' := 1
      /\ Nb' := new()
      /\ Snd(Pkb.B.{Pkb.B}_inv(Pks).Nb'.A.ctext4.{Nb'.A.ctext3}_inv(Pkb))
      /\ witness(B,A,nb,Nb')
      /\ wrequest(B,A,na,Na')

end role
```

```
role session (A, B     : agent,
              Pka, Pkb : public_key,
              Pks      : public_key) def=
  local SA, RA, SB, RB: channel (dy)

  composition

          iso3_Init(A,B,Pka,Pks,SA,RA)
       /\ iso3_Resp(B,A,Pkb,Pks,SB,RB)

end role
```

```
role environment() def=

  const ctext1, ctext2, ctext3, ctext4 : text,
        na, nb                         : protocol_id,
        a, b                           : agent,
        pka, pkb, pks, pki             : public_key

  intruder_knowledge={a,b,pks,pki,inv(pki)}

  composition

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

end role
```

```
goal

   %ISO3_Init weakly authenticates ISO3_Resp on nb
   weak_authentication_on nb

   %ISO3_Resp weakly authenticates ISO3_Init on na
   weak_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.