fixed version with weak authentication

Protocol Purpose

Sender invariance (authentication assuming that the first message is not tampered with)

Definition Reference

http://www.ietf.org/internet-drafts/draft-bradner-pbk-frame-06.txt

Model Authors

- Daniel Plasto for Siemens CT IC 3, 2004
- Sebastian Mödersheim, ETH Zürich

Alice&Bob style

```
A -> B: A, PK_A, hash(PK_A)
A -> B: {***tag1***,Msg}inv(PK_A), hash(PK_A)
B -> A: Nonce
A -> B: {***tag2***,Nonce}inv(PK_A)
```

Problems considered: 1

Attacks Found

None

Further Notes

Same as before, but specifying only weak authentication.

HLPSL Specification

```
role alice (A,B        : agent,
            SND,RCV    : channel(dy),
            Hash       : function,
            PK_A       : public_key,
            Tag1,Tag2  : text)
played_by A
def=

  local
    State      : nat,
    Msg        : text,
    Nonce      : text

  init State := 0

  transition

 1. State  = 0 /\ RCV(start) =|>
    State':= 2 /\ Msg' := new()
               /\ SND(B.{Tag1.Msg'}_inv(PK_A).Hash(PK_A))
               /\ witness(A,A,msg,Msg')

 3. State  = 2 /\ RCV(Nonce') =|>
    State':= 4 /\ SND({Tag2.Nonce'}_inv(PK_A))

end role
```

```
role bob (B,A        : agent,
          SND,RCV    : channel(dy),
          Hash       : function,
          PK_A       : public_key,
          Tag1,Tag2  : text)
played_by B
def=

  local
```

```
    State      : nat,
    Nonce      : text,
    Msg        : text

  init State := 1

  transition

 1. State  = 1 /\ RCV(B.{Tag1.Msg'}_inv(PK_A).Hash(PK_A)) =|>
    State':= 5 /\ Nonce' := new()
               /\ SND(Nonce')

 3. State  = 5 /\ RCV({Tag2.Nonce}_inv(PK_A)) =|>
    State':= 7 /\ wrequest(A,A,msg,Msg)

end role
```

```
role session(A,B        : agent,
             Hash       : function,
             PK_A       : public_key,
             Tag1,Tag2        : text)
def=

  local SND,RCV,SNDA,RCVA  : channel (dy)

  composition

     alice(A,B,SND,RCV,Hash,PK_A,Tag1,Tag2)
  /\ bob(B,A,SND,RCV,Hash,PK_A,Tag1,Tag2)

end role
```

```
role environment()
def=

  const
    a,b            : agent,
```

```
    f               : function,
    msg             : protocol_id,
    pk_a,pk_b,pk_i  : public_key,
    tag1,tag2       : text

  intruder_knowledge = {a,b,f,pk_a,pk_b,pk_i,inv(pk_i)}

  composition
     session(a,b,f,pk_a,tag1,tag2)
  /\ session(b,a,f,pk_b,tag1,tag2)
  /\ session(i,b,f,pk_i,tag1,tag2)
  /\ session(a,i,f,pk_a,tag1,tag2)

end role
```

```
goal

  %Alice weakly authenticates Alice on msg
  weak_authentication_on msg

end goal
```

```
environment()
```

References