ISO1 Public Key Unilateral Authentication Protocol

one-pass unilateral authentication

Protocol Purpose

A client authenticates himself to a server by sending a digital signature.

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}inv(PKs), Na, B, Text,{Na,B,Text}inv(PKa)
```

Problems considered: 1

Attacks Found

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

```
i     -> (a,6) : start
(a,6) -> i     : pka,a,{pka,a}inv(pks),na(a,6),b,ctext,
                 {na(a,6),b,ctext}inv(pka)
i     -> (b,4) : pka,a,{pka,a}inv(pks),na(a,6),b,ctext,
                 {na(a,6),b,ctext}inv(pka)
i     -> (b,7) : pka,a,{pka,a}inv(pks),na(a,6),b,ctext,
                 {na(a,6),b,ctext}inv(pka)
```

Further Notes

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

If one would like to use the same server public key for each session, then permutation on `Pks` should be avoided.

HLPSL Specification

```
role iso1_Init ( A,B : agent,
                 Pka, Pks : public_key,
                 Snd, Rcv : channel(dy))
played_by A
def=

 local  State: nat,
        Na   : text

 init  State := 0

 transition

   1. State = 0
      /\ Rcv(start)
      =|>
      State' := 1
      /\ Na' := new()
      /\ Snd(Pka.A.{Pka.A}_inv(Pks).Na'.B.ctext.{Na'.B.ctext}_inv(Pka))
      /\ witness(A,B,na,Na')

end role
```

```
role iso1_Resp (A, B: agent,
                Pks : public_key,
```

```
                Rec : channel(dy))
played_by B
def=

  local  State     : nat,
         Pka       : public_key,
         Na, Text  : text

  init  State := 0

  transition

   1. State = 0
      /\ Rec(Pka'.A.{Pka'.A}_inv(Pks).Na'.B.Text'.{Na'.B.Text'}_inv(Pka'))
      =|>
      State' := 1
      /\ request(B,A,na,Na')

end role
```

```
role session (A, B : agent,
              Pka  : public_key,
              Pks  : public_key) def=

  local SA, RA, RB: channel (dy)

  const na : protocol_id

  composition

          iso1_Init(A,B,Pka,Pks,SA,RA)
       /\ iso1_Resp(A,B,Pks,RB)

end role
```

```
role environment() def=
```

```
  const ctext    : text,
        a, b     : agent,
        pka, pks : public_key

  intruder_knowledge={a,b,pks,pka}

  composition

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

end role
```

```
goal

   %ISO1_Resp authenticates ISO1_Init 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.