IMSR: Improved Modulo Square Root

LPD (Low-Powered Devices) Improved MSR (Modulo Square Root) protocol is a key establishment protocol for secure mobile communications. It has been designed by Beller, Chang, and Yacobi in 1990s as an improvement of MSR. Namely IMSR overcomes a major weakness of MSR by including a certificate of the base station in the first message. Apart from this feature it is identical to the basic MSR protocol, and therefore does not address the problem of replay

Protocol Purpose

Key establishment protocol for secure mobile communications.

Definition Reference

- [BM98, pages 5-6]

Model Authors

- Graham Steel, University of Edinburgh, July 2004
- Luca Compagna, AI-Lab DIST University of Genova, November 2004

Alice&Bob style

```
B, M    : agent
PKb     : public key
SCm     : text
Nb      : text (fresh)
Cert(B) : message
X       : symmetric key (fresh)

1. B -> M : B, Nb, PKb, Cert(B)
2. M -> B : {X}PKb
3. M -> B : {Nb, M, SCm}X
```

The object `SCm` denotes the secret certificate of the mobile `M` which is issued by a trusted central authority. `Cert(B)` is the public certificate previously issued by some server for `B`. We assume `Cert(B) = {B.PKb}inv(PKs)`.

Notice that wrt MSR there is a twofold increase in the complexity of this protocol as compared to the basic MSR protocol. The mobile now calculates an additional modulo square to verify the base's certificate on receiving message 1. Upon receiving the final message, `B` decrypts it using the session key `X`, and checks that the value `Nb` is the same as the random challenge sent in message 1.

Model Limitations

The protocol would require the mobile `M` to send two sequential messages to the base station `B` in a row. We model such a situation by sending in one single transition the pair of the two messages.

Problems considered: 2

Attacks Found

None

Further Notes

The added public certificate and nonce exchange give some more protection. Boyd et al. [BM98] recommend moving the nonce and `M` into message 2.

HLPSL Specification

```
role imsr_Base(B, M     : agent,
               SCm      : text,
               PKb      : public_key,
               PKs      : public_key,
               Snd, Rcv : channel (dy))
played_by B
def=
```

```
  local State   : nat,
        X       : symmetric_key,
        Nb      : text,
        Package : message

  const  x : protocol_id

  init   State := 0

  accept State = 2

  transition

   1. State = 0
      /\ Rcv(start)
      =|>
      State' := 1
      /\ Nb' := new()
      /\ Snd(B.Nb'.PKb.{B.PKb}_inv(PKs))

   2. State = 1
      /\ Rcv({X'}_PKb.{Nb.M.SCm}_X')
      =|>
      State' := 2
      /\ wrequest(B,M,x,X')

end role
```

```
role imsr_Mobile(B, M     : agent,
                 SCm      : text,
                 PKs      : public_key,
                 Snd, Rcv : channel (dy))
played_by M
def=

  local State  : nat,
        PKb    : public_key,
        X      : symmetric_key,
        Nb     : text,
```

```
        Cert   : message

  const secx   : protocol_id

  init   State := 0

  accept State = 1

  transition

   1. State = 0
      /\ Rcv(B.Nb'.PKb'.Cert')
      /\ Cert' = {B.PKb'}_inv(PKs)
      =|>
      State'=1
      /\ X' := new()
      /\ Snd({X'}_PKb'.{Nb'.M.SCm}_X')
      /\ secret(X',secx,{B,M})
      /\ witness(M,B,x,X')

end role
```

```
role session(B, M           : agent,
             SCm            : text,
             PKb, PKs       : public_key) def=

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

  composition

       imsr_Base(B,M,SCm,PKb,PKs,SA,RA)
    /\ imsr_Mobile(B,M,SCm,PKs,SB,RB)

end role
```

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

```
  const b, m                                    : agent,
        kb, ki, ks                              : public_key,
        scm1, scm2, scm3                        : text

  intruder_knowledge = {b,m,scm2,scm3,i,ki,ks,inv(ki),
                        m,{i.ki}_inv(ks)
                       }

  composition

        session(b,m,scm1,kb,ks)
    /\  session(b,i,scm2,kb,ks)
    /\  session(i,m,scm3,ki,ks)

end role
```

```
goal

  % The established key X must be a secret between the base and the mobile
  secrecy_of secx

  % Authentication: base station authenticates mobile
  %IMSR_Base weakly authenticates IMSR_Mobile on x
  weak_authentication_on x

end goal
```

```
environment()
```

References

[BM98] Colin Boyd and Anish Mathuria. Key establishment protocols for secure mobile communications: A selective survey. *Lecture Notes in Computer Science*, 1438:344ff, 1998.