LPD: Low-Powered Devices

MSR: Modulo Square Root

LPD (Low-Powered Devices) 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. Such a protocol relies on a public key cryptosystem for which encryption is particularly efficient, at least in comparison to other public key cryptosystems. The specific public key cryptosystem employed is due to Rabin, in which encryption and decryption tantamount, respectively, to modulo squaring and extracting a modulo square root (MSR). MSR technique allows public key encryption to be implemented within the computational power of a mobile station.

Protocol Purpose

Key establishment protocol for secure mobile communications.

Definition Reference

- [BM98, page 4]

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
X    : symmetric key (fresh)

1. B -> M : B, PKb
2. M -> B : {x}PKb
3. M -> B : {M, SCm}x
```

The object `SCm` denotes the secret certificate of the mobile M which is issued by a trusted central authority.

Upon receiving `B`'s public key `PKb`, the mobile uses it to encrypt the session key `X`, and sends the encrypted message to `B`. The mobile also sends its identity and secret certificate encrypted under `X` to authenticate `X` to the base. The encryption in message 3 is carried out using a symmetric key cryptosystem. Since this encryption is negligible compared to the public key encryption in message 2, the computational effort at the mobile is effectively reduced to that of modulo squaring of the session key.

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

The public key of `B` is uncertified, thereby allowing anyone to masquerade as `B` (perceived as a serious threat in the emerging standards). Moreover replay of an old compromised session key allows masquerade of `M`. As a matter of fact, the following attack trace:

```
 i       -> (b,3) : start
 (b,3)   -> i : b,kb
 i       -> (m,4) : b,ki
 (m,4)   -> i : {x0(m,4)}ki,{m,scm1}x0(m,4)
```

suffices (i) to violate the secrecy of the established session key `X` and (ii) to make the base station `B` to believe talking with the mobile `M` while it is talking with the intruder.

HLPSL Specification

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

  local  State : nat,
         X     : symmetric_key

  init   State := 0

  accept State = 2

  transition

   1. State = 0
      /\ Rcv(start)
      =|>
      State' = 1
      /\ Snd(B.PKb)

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

end role
```

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

  local State  : nat,
        PKb    : public_key,
        X      : symmetric_key
  const secx   : protocol_id

  init   State := 0

  accept State = 1

  transition

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

end role
```

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

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

  const  x : protocol_id

  composition

          msr_Base(B,M,PKb,SCm,SA,RA)
       /\ msr_Mobile(B,M,SCm,SB,RB)

end role
```

```
role environment() def=

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

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

composition

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

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
  %MSR_Base weakly authenticates MSR_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.