(MS-)CHAPv2

Challenge/Response Authentication Protocol, version 2

Protocol Purpose

Mutual authentication between a server and a client who share a password. CHAPv2 is the authentication protocol for the Point-to-Point Tunneling Protocol suite (PPTP).

Definition Reference

[Zor00]

Model Authors

- Haykal Tej, Siemens CT IC 3, 2003
- Paul Hankes Drielsma, ETH Zürich

Alice&Bob style

We assume that the server `B` and client `A` share password `k(A,B)` in advance. The server and client generate nonces `Nb` and `Na`, respectively.

```
1. A -> B : A
2. B -> A : Nb
3. A -> B : Na,H(k(A,B),(Na,Nb,A))
4. B -> A : H(k(A,B),Na)
```

Model Limitations

Issues abstracted from:

- Message structure: As is standard, we abstract away from the concrete details of message structure such as bit lengths, etc. What is left after this abstraction contains several redundancies, however (at least in the Dolev-Yao model). We therefore eliminate these redundancies, retaining the core of the data dependencies of the protocol.

Problems considered: 3

Attacks Found

None

Further Notes

A cryptanalysis of this protocol in its full complexity can be found in [SMW99].

HLPSL Specification

```
role chap_Init (A,B   : agent,
                Kab   : symmetric_key,
                H     : function,
                Snd, Rcv: channel(dy))
played_by A
def=

  local State  : nat,
        Na, Nb : text

  const sec_kab1 : protocol_id

  init  State := 0

  transition
   1. State   = 0 /\ Rcv(start) =|>
      State' := 1 /\ Snd(A)

   2. State   = 1 /\ Rcv(Nb') =|>
      State' := 2 /\ Na' := new() /\ Snd(Na'.H(Kab.Na'.Nb'.A))
                  /\ witness(A,B,na,Na')
                  /\ secret(Kab,sec_kab1,{A,B})
```

```
   3. State   = 2 /\ Rcv(H(Kab.Na)) =|>
      State' := 3 /\ request(A,B,nb,Nb)

end role
```

```
role chap_Resp (B,A : agent,
                Kab : symmetric_key,
                H: function,
                Snd, Rcv: channel(dy))
played_by B
def=

  local State  : nat,
        Na, Nb : text

  const sec_kab2 : protocol_id

  init  State := 0

  transition
   1. State   = 0 /\ Rcv(A') =|>
      State' := 1 /\ Nb' := new() /\ Snd(Nb')
                  /\ witness(B,A,nb,Nb')

   2. State   = 1 /\ Rcv(Na'.H(Kab.Na'.Nb.A)) =|>
      State' := 2 /\ Snd(H(Kab.Na'))
                  /\ request(B,A,na,Na')
                  /\ secret(Kab,sec_kab2,{A,B})

end role
```

```
role session(A,B: agent,
             Kab: symmetric_key,
             H: function)
def=

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

  composition
```

```
           chap_Init(A, B, Kab, H, SA, RA)
       /\  chap_Resp(B, A, Kab, H, SB, RB)
end role
```

```
role environment()
def=

  const a, b          : agent,
        kab, kai, kbi : symmetric_key,
        h             : function,
        na, nb        : protocol_id

  intruder_knowledge = {a, b, h, kai, kbi }

  composition
        session(a,b,kab,h) /\
        session(a,i,kai,h) /\
        session(b,i,kbi,h)

end role
```

```
goal

 %secrecy of the shared key
 secrecy_of sec_kab1, sec_kab2

 %CHAP_Init authenticates CHAP_Resp on nb
 authentication_on nb
 %CHAP_Resp authenticates CHAP_Init on na
 authentication_on na

end goal

environment()
```

References

[SMW99] Bruce Schneier, Mudge, and David Wagner. Cryptanalysis of microsoft's PPTP authentication extensions (MS-CHAPv2). In *CQRE: International Exhibition and Congress on Secure Networking – CQRE [Secure]*, 1999.

[Zor00] G. Zorn. RFC 2759: Microsoft PPP CHAP Extensions, Version 2, January 2000. Status: Informational.