(MS-)CHAPv2

Challenge/Response Authentication Protocol, version 2

Protocol Purpose

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: cha14(Rne)1(l(d)1(y))1())-9431-14.446[pl)1(ay)1(ed_)1(by)-14(

                tra14(Rsit)1(io)1(n)612)tate   = 0\ Rcv(start)>
                   State’ nd(A)

                2.tate   = 1\ Rcv(11(’))-S>
```

```
3. State   = 2 /\ Rcv(H(Kab.Na)) =|>
```