H.530: Symmetric security procedures for H.323 mobility in H.510

Original version

Protocol Purpose

Problems considered: 3

Attacks Found

A replay attack, as AuF's reply to the authentication request from VGK does not contain enough information that VGK can read. The attack works by first observing a session between honest agents and then replaying messages from this session to VGK, posing both as MT and AuF. Use option sessco to find this attack with OFMC. Another attack recently discovered with OFMC is based on the fact that VGK

```
    ZZ_VA      : symmetric_key,
    NIL,G      : text)
played_by VGK def=

  local
    State           : nat,
    GX,Key,Key1’304-105814(na)1my1’3sym
```

```
 /\ authenticationFacility(MT,VGK,AuF,SND,RCV,F,ZZ,ZZ_VA,NIL,G)
 /\ visitedGateKeeper(MT,VGK,AuF,SND,RCV,F,ZZ_VA,NIL,G)

end role
```

```
role environment()
def=

  const
    a,b,auf      : agent,
    f            : function,
    kekekea,b,tint
```