GDOI PROOF OF POSSESSION

Catherine Meadows
Naval Research Laboratory
Code 5543
Washington, DC, 20375
meadows@itd.nrl.navy.mil

HOW POP WORKS IN GDOI

- When member joins a group, may get a new identity
  - **This identity is (or is associated with) a public key**
- Member needs to prove possession of identity to the Group Controller/Key Server (GCKS)
  - **Member signs hash("pop" | Ni | Nr)**
  - **Ni = member's nonce**
  - **Nr = GCKS's nonce**
  - **"pop" = string identifying this is POP message**
- GCKS can also send certificate with new GCKS ID to member
  - **In that case, also needs to sign proof of possession message**

THE PROBLEM

- No indication of who is signing the POP
- You know it’s the possessor of the new ID, but who is that?

AN ATTACK

Suppose that I is a GCKS that wants join a group managed by another GCKS, B.

Suppose that I doesn't have the proper credentials to join B's group.

Assuming that A's credentials work for both I's group and B's group, I can trick a member A who does into supplying them, as follows.

1. A --> I : HDR*, HASH(1), Ni, ID A requests to join I's group, sending a nonce Ni

1.' I_member --> B : HDR*, HASH(1)', Ni, ID' I requests to join B's group, forwarding A's nonce Ni

2.' B --> I_member : HDR*, HASH(2), Nr', SA' B responds to I with its nonce Nr'

2. I --> A : HDR*, HASH(2)', Nr', SA I responds to member A, but using B's nonce Nr'

3. A --> I: HDR*, HASH(3), CERT(for A's ID in group), POP = S_A(hash(Ni,Nr'))
A responds to I with a POP taken over A's and B's nonce

3.' I_member --> B: HDR*, HASH(3), CERT(for A's ID in group), POP = S_A(hash(Ni,Nr))
I as a member responds to B, using A's CERT and POP

4. B --> I_member : HDR*, HASH(4), KD
B sends keying information to I under impression the identity in A's certificate belongs to I

ALSO …

- Can perform similar attack on GCKS's POP
  - **Allows attacker to impersonate GCKS**
- Can compose attack on member's POP with attack on GCKS's POP
  - **Allows attacker to impersonate GCKS to member and member to GCKS**

HOW TO PROCEED?

- Attack is on an option
- Requires member's credentials be good for more than one group
- Not necessary to revise current RFC, but fix should appear in GDOIv2
  - **One suggestion: write draft describing attack and fix**

TWO POSSIBLE FIXES

- Need to have way of including principal's old ID
- Fix 1
  - **Replace POP info with hash("pop" |ID_i| Ni | Nr)**
  - **ID_i is ID GCKS knows group member by**
  - **Drawback: GCKS may know member by more than one ID**
- Fix 2
  - **Replace POP with hash("pop" |K| Ni | Nr)**
  - **K is IKE key shared by GCKS and member**
  - **Drawback: increases exposure of key**