Multicast Router Key Management Protocol (MRKMP)

draft-hartman-karp-mrkmp-01
Sam Hartman Painless Security
Dacheng Zhang, Huawei
Election Protocol

• Election protocol improved to address comments since IETF 79
• Re-design the election protocol of MRKMP
• Objectives of the election protocol:
  – Pick a router as a GCKS
  – Under attacks, the best candidate does not have to be selected
  – Once the election has been concluded, keep using the GCKS until it fails
Election Protocol in -00

State Machine

Initial

Member

GCKS

Router A

A’s state = Initial, priority = low

A->group: state = init, priority = low

B’s state = Initial, priority = high

B-> group: state = init, priority = high

Router B

A’s state = Member, priority = low

B’s state = GCKS, priority = high

Time Delay

t1
t2
Main Attack

• An attacker can send new announcements to keep the election going. (convergence can be very slow)

• Clues about attacks:
  – An election can conclude but authentication fails
  – An election takes too long
Proposal

• Detect the attacks, and when an attacker is detected, use a slower strategy
  – In the slower strategy, try to find the routers which can be authenticated to
  – Build the tree of these routers and pick one as the key server

• Introduce new States, Validate, GCKS2, and Follower
• When an attack is detected, an Initial state transmits its state to GCKS2 or Follower. Otherwise, to GCKS or Member
• A GCKS2 router only distributes KEKs but does not distribute protocol master keys
Initial State

- Routers send initial announcements to show its existence
- Under following condition, transfer to Validate
  - Receive a GCKS or a GCKS2 announcement (put the sender into the candidate list before the state transmission)
  - After the initial timer expires, the candidate list is not empty
- If the list is empty, after the initial timer expires, transfer to GCKS
Validate State

- Authenticate the most preferred entry in the candidate list
  - If the one cannot be authenticated to, then there is an attacker. Transfer to the slower strategy

- If no authenticated and more preferred router is found during a certain period, transfer the state to GCKS2 and keep looking for the more preferred one
GCKS2

• Generate a KEK and distribute it to its followers
• Keep listening the GCKS or GCKS2 announcements, try to find more preferred routers and authenticate to them
Follower

• When an Initial router receives an GCKS2 router, it can transfer its state to Follower after authenticating to the GCKS2 router
• In a certain period, ignore any announcement from other routers