Multicast Routing Key Management Protocol

Sam Hartman
Dacheng Zhang
IETF79
draft-hartman-karp-mrkmp
Objectives

• Provide automated key management for routing protocols such as OSPF and IS-IS
• Use same credentials and similar approach for unicast key management
• Separate key management from actual routing protocols
Threat Model

• Insider attacks are out of scope
• Every member of the group can take on the GCKS role
• Groups are small and eviction rare
Credentials

• Solution should be independent of credential types
• Credentials may be preshared keys, asymmetric keys, PKI or something else
• No assumption of a PKI or any asymmetric keys
Starting from Known Technologies

• Based on GDOI for multicast operation
• Based on IKEv2 for base key management
• Some changes and alignment are required
Overview

• Elect a GCKS from available candidates
• All nodes perform unicast authentication to the GCKS and get initial key download
• GCKS may provide periodic updates
Election Protocol

State Machine

Member → GCKS → Initial

Router A

A’s state = Initial, priority = low
A->group: state = init, priority = low

Router B

B’s state = Initial, priority = high
B-> group: state = init, priority = high

A’s state = Member, priority = low

Time Delay

t1
t2
Election Constraints

• Objective: elect a valid member of the group as GCKS
• Attackers may force the outcome of the election
• Attackers should not be able to force a DOS
• Election is insecure; secure confirmation of candidate validity after
Initial Exchange

Router A

sa_init: HDR, PPSAi, KEi, Ni

sa_init_r HDR, PSAr, KEr, NR, [CERTREQ]

sa_init2: HDR, SK { IDi, IDr, AUTHSTUFF, GSAi}

Router B

sa_init2: SK { IDr, AUTHSTUFF, GSAr}
Key Update

Router B

b-> group: KEK{ GSAr}

Router A

Router N

Group
Questions