IETF88-PIM

Secure IGMP/MLD

draft-atwood-pim-sigmp

draft-atwood-mboned-mrac-req
draft-atwood-mboned-mrac-arch

J. William Atwood
Bing Li
Concordia University, Montreal

Overview

- Exploring the area of Receiver Access Control for IP Multicast
  - Subtitle: Making money using IP Multicast
  - Covers **some** of the same concerns as those of the "well-managed multicast" work that was presented in MBONED three years ago
  - **much** smaller scope of interest
  - MBONED: "application" level drafts
  - PIM: "network" level drafts

Two Assumptions

- The End User (EU) acquires a “ticket” from a “Merchant” (or anyone else) containing:
  - Session Descriptor
  - Secure End User authentication
  - Possibly, an encryption key for the data stream
- The “Network Representative” has information on how to validate a “ticket” or assess the authorization of the EU or EU Device
- This makes the discussion today independent of the business model in use by the NSP and/or CP
- It restricts the scope of the work

Two levels of interaction

- Application Level
  - EU presents the “ticket”
  - Goal: Join the group
- Network Level
  - End User Device issues IGMP/MLD

- To ensure that only legitimate subscribers get access
  - MUST be secure at Application Level
  - MUST be secure at Network Level

Two Approaches

- Solution 1
  - Carry the “ticket” in an extended network-level join exchange
    - The security of the two levels is implied by the fact that they are carried in a single level of message exchanges, which are secured
- Solution 2
  - Provide separate secure application level join and secure network level join functions, along with a method for explicitly coordinating them

Extending IGMP

- Long history of attempts to extend IGMP
  - All of them abandoned
  - All were “restricted” solutions
    - Based on a particular version of IGMP, -OR-
    - Proposed a limited set of authorization methods
  - List of citations in the draft
- None of these attempts considered “accounting” specifically

Securing IGMP/MLD

- One IRTF Internet Draft on securing IGMP
  - Once a device established a secure relationship with its router, it was allowed to send a join for ***any*** group.
- RFC 3376 suggests using AH to secure IGMP packets
- RFC 3810 is silent on the issue of securing MLD packets
- None of these attempts considered “accounting” specifically
  - No need to deploy the solution if accounting is unnecessary!

Approach

- We choose Solution 2
  - Reasons are in draft-atwood-mboned-mrac-req
- The Application-level requirements and the Interaction requirements in mrac-req are met in such a way that the End User and the NSP Representative will share a key
- This key can be used to derive keys for protecting MLD/IGMP
- A set of Network-level requirements remains

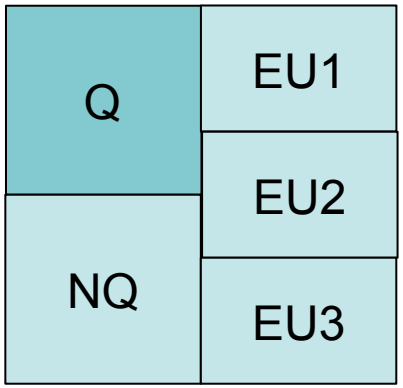
Requirements

- Network level constraints (for secure IGMP/MLD)
  - Maximum Compatibility with MLD and IGMP
  - Group Membership and Access Control
  - Minimal Modification to MLD/IGMP
  - Multiple Network Level Joins for End User Device
  - NSP Representative Differentiates Multiple Joins
  - Network Level Interaction must be Secured

Open vs Secure Groups

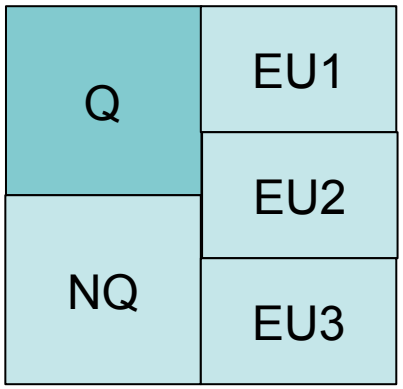
- Open Group
  - No access controls
  - Operations will follow standard IP multicast rules (3376 or 3810)
- Secured Group
  - Access controls to prevent an unauthorized EU from accessing the group
  - Additional operations are needed
  - IGMP/MLD exchanges are protected with IPsec, using the derived keys

Unsecure Query



GQ V2, V3

224.0.0.1
No group



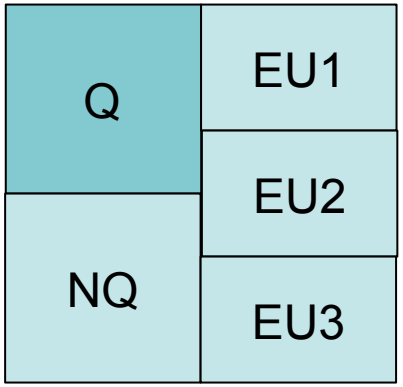
GSQ V2, V3
GSSQ V3

G_IP
Single group

Source

Destination

Secure Query



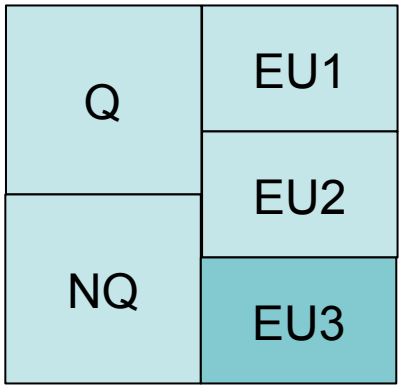
GSQ V2, V3
GSSQ V3
Secure

G_IP
Single group

IGMP v2/v3 Query

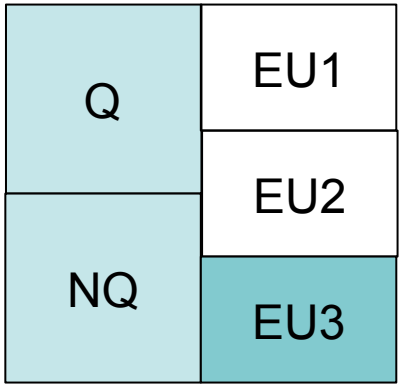
- The GQ is an “open” solicitation, for all groups, and so cannot be secured with information that is specific to one group. So, it has no “secure” form.
- The GSQ (v2 and v3) and GSSQ (v3 only) are specific to a group, and so can be secured with parameters that are specific to that group. No change is necessary to the packet format; we only need to protect the packet with IPsec.

Unsecure Report



R V2

Unsecure
Suppression
G_IP
Single group



R V3

Unsecure
NO suppression
224.0.0.22
Multiple groups

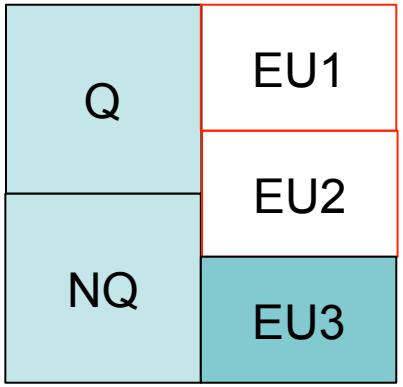
IGMP v2/v3 Report

- The details of the v2 report and the v3 report are quite different, because different design decisions were made on how to minimize traffic:
  - In v2, a Report contains only information about one group, but identical reports from other hosts should be suppressed.
  - In v3, multiple groups may be contained in a single Report, which is sent to a common address (224.0.0.22)

Secure IGMP v2/v3 Report

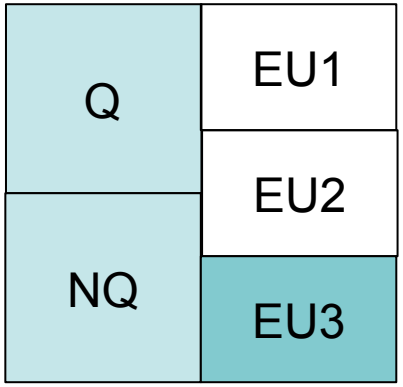
- Since the cryptographic protection must of necessity be specific to a group,
  - We cannot use address 224.0.0.22
  - We cannot have multiple groups in a Report message
- We are interested in minimum change to IGMP
  - Our solution requires no change to the packet format
- We are interested in maximum compatibility
  - Our solution does not change the semantics of IGMP for “open” groups

Secure Report



R V2

Secure
NO suppression
G_IP
Single group



R V3

Secure
NO suppression
G_IP
Single group

Multicast Security Associations for Secure IGMP

- Many distinct Multicast Security Associations are required on each network segment:
  - One with Q as the sender, and NQ plus the admitted members as receivers
  - One for each legitimate participant EU, with the EU as the sender, and NQ plus Q as the receivers
  - All are uni-directional, as defined in RFC5374

Three external problems

- Three problems are solved in a different document:
  - Determining the keys for these MSAs
  - Determining the Security Parameter Index to use
  - Distributing the keys and the SPIs to the participants who need them

Results

- Secure Authentication of IGMP
- Assuming that the keys are derived from the upper-level exchanges, the IGMP authentication and authorization is tied to the “ticket” of the End User
- Minimal modification of IGMP semantics, and no modification of IGMP packet format
- Compatible with all currently deployed versions of IGMP

Documents

- Issued
  - MRAC Requirements
    - draft-atwood-mboned-mrac-req
  - MRAC Architecture
    - draft-atwood-mboned-mrac-arch
  - Secure IGMP
    - draft-atwood-pim-sigmp
- To Come
  - Using PANA+EAP to achieve the MRAC
  - Secure MLD
  - GSAM (coordination of Secure IGMP end points)

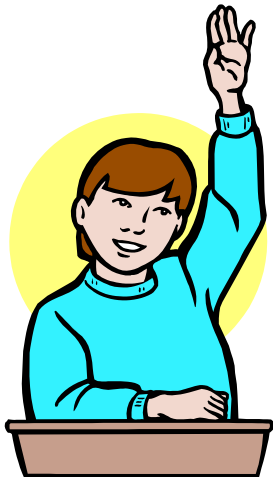
Acknowlegment

- Salekul Islam contributed significantly to mrac-req and mrac-arch

Next Steps

- Request for feedback (on the list or elsewhere)
- Eventual adoption of all three -pim documents as WG documents

Thank You!



Questions?