IP Multicast Receiver Access Control

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

J. William Atwood
Bing Li
Concordia University, Montreal
Salekul Islam
United International University, Dhaka
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
Trust Relationships: Unicast

- CP
- CS
- NSP
- EU
- EUD

- Red arrows: Purchasing
- Green arrows: Data Delivery
Trust Relationships: Multicast

Diagram showing relationships between CP, CS, NSP, EU, EUD with arrows indicating purchasing and data delivery.
Trust Relationships: Multicast, Re-established

CP

NSP

EU

CS

EUD

EUD

NSP Representative

Purchasing

Data Delivery
Problem Size:
mboned-maccnt-req

Covers various business models
Constraint: only one user on a physical link

AAA
QoS

Purchasing
Data Delivery
Problem Size: Other work in my lab

AAA
No QoS

General business model
N users on link

CP

Purchasing

Data Delivery

MR

FI

EUD

EU

EUD

NSP

2013-11-04
Two Assumptions

- The End User (EU) acquires a “ticket” from the 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
Problem Size: Today’s Discussion

- AAA
- MR
- FI
- CP
- EU
- EUD
- NSP

Connections:
- CP to AAA
- CP to NSP
- NSP to EU
- EU to EUD
- EU to EUD
- EU to EUD
- EU to EUD

Arrows indicate:
- Purchasing
- Data Delivery
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
  - A list of citations is 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!
Goals

- List the requirements on a set of mechanisms that
  - allow the Network Service Provider to act on behalf of the Content Provider
  - meet the access control and revenue generation goals
  - remain as independent as possible from the specific business model in use

- Specify an architecture that meets these goals
We explore Solution 2

- Separate joins and explicit coordination

Thus, the constraints fall naturally into three categories:

- Application-level constraints
- Network-level constraints
- Interaction constraints
Requirements

- Application level constraints
  - Authenticating and Authorizing Multicast End Users
  - Group Membership and Access Control
  - Independence of Authentication and Authorization Procedures
  - Re-authentication and Re-authorization
  - Accounting
  - Multiple Sessions on One Device
  - Multiple Independent Sessions on a LAN
  - Application Level Interaction must be Secured
Network level constraints

- 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
Interaction constraints

- Coupling of Network and Application Level Controls
- Separation of Network Access Controls from Group Access Controls
**Building Blocks**

- **AAA**: A general framework for managing access to networks, based on RADIUS and Diameter

- **EAP**: A general framework for negotiating a method for authenticating users
  - Some methods allow mutual authentication
  - Typically used for access to the “entire network”
  - Can be adapted to manage access to multicast groups
PANA: A “lower layer” for EAP, between the EUD and the NSP

- Can be used to create a key, known to the PANA Client (PaC) and the PANA Authentication Server (PAA) (= NSP Representative)
- Enforcement is done by an Enforcement Point (EP)

IGMP/MLD: Network-level access control for IP Multicast

- Unsecured (in standard multicast)
IP Security (IPsec): Protocols and methods for establishing the authenticity, integrity, and other cryptographic properties of IP datagrams

- Can be used to secure IGMP/MLD
- We call this secure form of IGMP/MLD Secure IGMP (SIGMP) or Secure MLD (SMLD)
Results

- Secure Authentication of the End User

  Authorization is then possible using standard AAA interactions within the NSP

- A shared key is generated, which can be used to derive the necessary keys for protecting the IGMP/MLD exchanges
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)
Next Steps

- Request for feedback (on the list or elsewhere)

- If this work is found useful, we request a liaison statement to PIM WG asking for the SIGMP/SMLD work to be done.
Thank You!

Questions?