End User Identification

J.W. Atwood, S. Islam

Mboned Working Group

2007/07/25

bill@cse.concordia.ca

Overview

- This is work that has been underway since well before the mldauth-ps document was published.
- We have worked out (and validated) a solution using IGMP+EAP, which should also be applicable to MLD.

IGMP-AC

- Problem is to correlate the IGMP join request with the authorizing of the End User to join the group.
- Solution is to extend IGMP to carry the authorization information.

Secure/Open groups

- It is necessary that any solution not impact the current operation of IGMP
  - If a group does not need security, standard IGMP interactions should continue to work.
  - If a group must be secured, then the additional interactions will happen.
  - IANA could be asked to assign a set of multicast addresses for Secure Group activities

Message Interactions

- End Host makes request to join, using IGMP-AC. End User has supplied authentication/authorization information for transport in IGMP-AC packet
- Access Router forwards this information inside a Diameter packet to the AAA Server (AAAS)
- AAAS makes the decision, and returns the result

Three new IGMP messages

- auquery: Authentication Unicast Query
  - From AR to Host
- areport: Authentication Report
  - Authentication parameters
  - From Host to AR
- aresult: Authentication Result
  - From AR to Host

Three new Diameter Messages

- Request()
  - Is this a secure group?
  - Is this user allowed?
- Answer()
  - Yes/No
  - Directions for recording accounting
- Account()
  - To provide accounting summary

Initial version

- Simple password authentication, as an example
- Full state diagrams developed for the End Host, the Access Router, and the AAA Server
- Then the interactions were validated using SPIN (a model checker)
- Published at LCN 2006

Subsequent version

- Full EAP support End User <-> AR and AR (NAS) <-> AAAS
- Use of EAP-IKEv2, as an example
- Validated EAP-IKEv2 in pass-through mode using AVISPA (since it is a validation of the use of security protocols)
- Paper is in preparation
- In future, validate other EAP methods using AVISPA

Policies are necessary

- Not efficient to keep information about all (potential) End Users in all Access Routers
- Access Router simply forwards information to AAAS for decision, and then accounts for resource usage
- Of course, the decision to gather accounting is another policy parameter

Sender Authentication (1)

- Of course, the sender(s) to the group need to be authenticated. This problem is harder, because there is no “sender join” in IP multicast.
- We trigger a sender authentication with an initial packet to the group (this packet may be empty)

Sender Authorization (2)

- An exchange with the sender’s AAAS is used to validate the sender
- A PANA session between the sender and the Access Router
- To be published at LCN 2007

Implications for the I-D

- Broaden it to include IGMP and MLD
- Ensure that sender issues are addressed (either here or in a separate document)

Papers

- J.W. Atwood, “An Architecture for Secure and Accountable Multicasting”, LCN 2007
- S. Islam and J.W. Atwood, “A Framework to Add AAA Functionalities in IP Multicast”, AICT 2006
- S. Islam and J.W. Atwood, “A Policy Framework for Multicast Group Control”, P2PM 2007
- S . Islam and J.W. Atwood, “The Internet Group Management Protocol with Access Control (IGMP-AC)”, LCN 2006
- S . Islam and J.W. Atwood, “Sender Access Control in IP Multicast”, LCN 2007
- S . Islam and J.W. Atwood, “End User Authentication, Authorization and Accounting in Multicasting”, in preparation
- S . Islam and J.W. Atwood, “User Access Control for Inter-Domain Multicast Groups”, in preparation
- (Requests for copies will be welcome. mailto:bill@cse.concordia.ca)