

# IETF92-MBONED



## Secure and Accountable AMT

J. William Atwood

Teja Malla

Abonti Ferdous

*Concordia University, Montreal*

# AMT is not secure



- ❑ Possible for an intruder to force disconnection of an AMT Gateway
  - Just issue AMT Membership update Leave/Done
- ❑ Possible for an intruder to masquerade as an AMT Relay
  - Just advertise on the anycast address
- ❑ No way to verify the legitimacy of a client
- ❑ Shown in paper at LCN 2011

# Multicast Receiver Access Control (MRAC)



- ❑ Has been presented to MBONED previously
- ❑ Allows verification of the legitimacy of a client
- ❑ Based on the use of EAP for authentication and PANA for transport of EAP packets, plus a “secure” form of IGMP
- ❑ To make MRAC useful in an AMT environment, we need a “secure” AMT
- ❑ Implies integration of MRAC and AMT

# Traditional AMT



- ❑ AMT Gateway contains an IGMP proxy
  - To capture the IGMP messages and forward them to the AMT Relay
- ❑ AMT Relay contains an IGMP proxy
  - To receive forwarded IGMP messages and send them on to the multicast-enabled router
- ❑ A tunnel exists between AMT Gateway and AMT Relay

# Integrating MRAC and AMT



- ❑ Add proxies to AMT Gateway and AMT Relay
  - EAP proxy
  - PANA proxy
  - Secure IGMP/MLD proxy
- ❑ Then formally validate that the security of the augmented AMT meets the same goals as those for MRAC in a “native” multicast environment
  - Assumes a “secure” AMT
  - Paper to be presented at ICN 2015 in April

# Secure AMT



- ❑ Must carry the additional packet types needed
- ❑ Have to ensure that
  - AMT peers can validate each other
  - A secure path is provided for the carried messages
- ❑ Work is in progress
  - Design the set of interactions
  - Validate the security formally

# AMT in Linux and Android



- ❑ Original implementation of AMT was written by Tom Pusateri at Juniper, for Free BSD
- ❑ Ported to Linux at University of Texas at Dallas, with support from Cisco
- ❑ We have fixed a few nits in the Linux version, and are porting it to Android.

# Papers



- Ali Salem and J. William Atwood, “Formal Validation of the Security Properties of AMT's Three-way Handshake”, Proceedings of the 36th Annual IEEE Conference on Local Computer Networks (LCN 2011), Bonn, Germany, 2011 October 4--7, pp. 227--230. DOI: 10.1109/LCN.2011.6115195
- Veera Nagasiva Tejeswi Malla and J. William Atwood, “Multicast Receiver Access Control in the Automatic Multicast Tunneling (AMT) Environment, accepted for presentation at the Fourteenth International Conference on Networks (ICN 2015), Barcelona, Spain, 2015 April 19--23.

# IETF Documents Issued



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

# Thank You!



Questions?