

Updates on Receiver Access Control



Haixiang He, Nortel Networks

Thomas Hardjono, Verisign

Brad Cain, Cereva Networks

Contact: haixiang@nortelnetworks.com



What we have done!

- Submit Two Drafts
 - Simple Multicast Receiver Access Control:
draft-irtf-gsec-smrac-00.txt
 - Uploading Authentication Information Using IGMPv3:
draft-he-magma-igmpv3-auth-00.txt
- First draft talks about access control theory and targets for GSEC.
- Second draft talks about the changes of IGMPv3 and targets for MAGMA.



Token Replay

- Replaying a token does not gain anything if the token's legal owner still subscribes the multicast traffic.
- Replaying a token between the expiration time of the token and the time the legal owner stops subscribing the same traffic is an issue.
- This maybe tolerable since the state records are already created and traffic is already flowing.



Token Replay Cont.: Solution

- Propose to use another public-key pair.
- Put the public key in the access token to replace the host IP.
- Distribute the private key along the access token securely to a host.
- A host signs its IGMP requests and also attaches its signature to its IGMP requests.
- Routers use the public key in the access token to read the signature.



Usage of Host IP

- Recent comments in the mailing list suggest to use prefix.
- Prefix does not work well for switch network where different ports may have the same prefix.
- How to use the token if a host reboots or changes its IP address?