Anycast security requirements

Lakshminath Dondeti
Thomas Hardjono
Brian Haberman

SMuG meeting, March 18, 2001
IETF-50, Minneapolis, MN

Introduction to anycasting

- Deliver packets to “topologically nearest” network element with the address
- Provides fault-tolerance
- Two packets sent to anycast address may reach different servers
  - Sending an anycast request is an atomic operation

Anycast routing

- Anycast routing [RFC 1546]
  - Anycast servers use
    - ARP or
    - Link-level multicast for advertisements and listening
  - Forwarding is similar to unicasting in the network
  - Last-hop routing is similar to that in multicasting

IPv6 anycast routing

- IPv6 anycast [RFC 2373]
  - Does not distinguish between unicast and anycast addresses during routing
  - The interface configured with the anycast address knows about it
  - A server receiving an anycast packet needs to put its own unicast address as sender address in the replying packet

Issues in anycast security

- Similar issues as in multicast security and more!
- Unauthenticated server advertisements
- Anycast server authenticity
- Secure anycast communications
- Connection and SA migration
  - For fault-tolerance

Anycast server advertisements

- Routers have no way of knowing legitimate servers
- Any host can advertise itself as an anycast server
  - To provide false information
  - "Attract" anycast packets but not reply
    - DOS attack
- Solution: Anycast server registration

Anycast server authenticity

- A client has no way of telling whether the replying server is legitimate
- Source address in an anycast reply packet is NOT the anycast address
  - It is server's unicast address
- Solution: Server's "group authentication" along with the reply

Secure anycast communication

- Private anycast communication
- Server authentication (addressed separately in the previous slide)
- Solution: An IPsec counterpart for anycast
  - We may draw from group security work

Connection and SA migration

- Anycast provides a fault-tolerant service discovery mechanism
- We propose to extend this notion to support persistent connections
- Need connection migration mechanism
  - Available in the literature
- For security, we need SA migration!

Proposed solutions

- Anycast server registration
- Server authentication
  - Anycast group authentication
- IPsec counterpart for anycast security
  - May not be too different from IPsec
- SA migration to support secure anycast connection migration

Anycast server registration

- Essentially a group access control problem
- Access control verification by routers before server advertisement
- As in multicast group membership control there are two options
  - Inclusion or exclusion ACLs
  - Authorization certificates

Anycast access control

- Each router maintains
  - ACLs for all supported anycast groups
  - (server, group) authorization lists
    - Proposed in an I-D about MLD for anycast
  - A list of “authorization tokens”
    - Proposed by Hardjono and Cain
    - Routers maintain valid token lists (VTL)

List-based access control

- Issues in maintaining ACLs, VTLs
  - Need distribution and updating mechanisms
  - Routers may filter unnecessary information where applicable
- VTL specific issues
  - Prospective anycast servers need to contact an AGC and obtain a valid token
    - Anycast group controller (AGC)

Authorization certificates

- Tokens are verifiable by participating routers only
- Auth certs are verifiable by anyone
  - More expensive though
- An AGC issues certs after verifying access control
  - All routers should have the AGC's certificate

Server authentication

- Client needs to know that it is hearing from a legitimate anycast server
- Servers need to produce a cert which proves that they belong to an anycast group
  - Signed by AGC
  - Signed by individual routers
    - Routers' certs are signed by AGC

IPsec for secure anycast communication

- IKE negotiations
  - Initiator (client) sends service location request to anycast address
  - Responder (server) replies with source address as its unicast address
  - Rest of the negotiations do not change
- We lose the fault-tolerant nature of anycast service location!
- Further details TBD

Extending anycast services

- Anycast provides fault-tolerant service discovery
- Propose to extend the notion to provide persistent anycast connections
- We need a mechanism for anycast connection migration
  - Anycast becomes stateful!
- For security, we need SA migration also

Connection and SA migration

- To the client, anycast provides a service
- SA migration
  - Notion of anycast group becomes stronger
  - Transfer SA parameters between members of an anycast group

Summary

- Anycast security is a concern
  - IPNG WG, DNS discovery design team
- Secure server registration
  - MLD for anycast group management
- Anycast server authentication
- Secure anycast communication
- SA migration for persistent anycast connection support