Secure Multicast Routing for Disseminating Active Code

J.J. Garcia-Luna-Aceves
Brad Smith
Lori Flynn

Jack Baskin School of Engineering
University of California, Santa Cruz

Active Service Deployment

- a standard node environment
- the service protocols themselves
- a service discovery and bootstrap mechanism
- a service distribution mechanism

Service Distribution Mechanism

- Must be:
  - secure - authorization of node to run code
  - reliable - guarantee that nodes needing code receive it
  - efficient - effect of code size on distribution
  - scalable - number of copies sent per link
- Two styles of addressing nodes
  - in-band - carrying code in active service messages
  - out-of-band - distribute code separate from active service
- Two forms for packaging code
  - directly, sending the code itself
  - indirectly, sending an address for the code (e.g. URL)

Service Distribution Mechanism (cont.)

- Each has strengths and weaknesses
  - code in-band - limited security, reliable, not efficient, scalable
  - code out-of-band - secure, reliable, not efficient, doesn’t scale
  - URL - secure, reliable, efficient, doesn’t scale
- Alternative code package: multicast group ID

Active Packet Dissemination Protocol (APDP)

- Secure, reliable multicast
- Active nodes join group to receive code
- Efficient - code defined with multicast group address
- Scales well - one copy of code per link

Secure Multicast - General Mechanisms

- per-group key
- access control and key distribution servers
- hosts and routers get key to carry group
- re-key on member join/leave and on policy change

Secure Multicast - Challenges

- key distribution
- reliability
- secure infrastructure - authentication of routers
  - multicast routing uses unicast routes to build trees
  - security policies must be consistent across unicast routing and all multicast groups
  - this clearly is not acceptable.

Sender-Initiated Solution

- PIM-DM with RBP tree-building mechanism
- Modified PIM-DM to not depend on unicast routes
- Does not guarantee shortest-path spanning tree
- Does guarantee per-group "trusted-path spanning tree"
- Currently working on receiver-initiated solution

Team 4 Integration

- Seraphim
  - clearly plays a role here - not what initially thought
  - initially - router authorize neighbor for group
  - should be - ACS authorize router for group
  - ...except for the multi-level rules
- CANES
  - need a stable, simple PIM-DM implementation
- Maude
  - specification and verification of reliable multicast protocol
  - used tree-building mechanism to secure PIM-DM