A taxonomy of multicast security issues

draft-irtf-smug-taxonomy-01.txt

Ran Canetti, IBM Research
Benny Pinkas, Intertrust Tech.

Goals of the draft

- To identify prominent scenarios for usage of IP multicast.
- To identify security concerns in IP multicast.
- To survey relevant work on secure multicast:
  - Find out what's out there
  - Identify areas where solutions are unsatisfactory

Multicast communication:

Whenever there are multiple recipients

- Typical applications:
  - File and software updates
  - News-feeds
  - Multimedia broadcasts (streaming):
    - Live
    - Pre-recorded
  - Virtual conferences, town-hall meetings
  - Multiparty gaming

Group characteristics

- Number of sources, receivers
- Membership dynamics
- Bandwidth and latency requirements.
- Duration
- Physical separation
  (network topology and political separation)

Security requirements

- Limiting access to group communication:
  - Long-term secrecy
  - Ephemeral access restriction
- Authentication:
  - Group
  - Source
- Anonymity
- Availability (against denial of service and flooding attacks)
- Protection against illegal re-distribution

Trust issues

- A solution may put trust in a “centralized group controller” to:
  - generate keys properly
  - distribute keys properly
  - no trust at all (all work done collectively by group members)
- A solution may trust group members to:
  - not impersonate group members
  - not re-distribute keys
  - no trust at all

Performance parameters of security solutions

- Time to verify and decrypt data
- Time to authenticate and encrypt data
- Communication bandwidth overhead
- Key set-up and refreshment overhead
- Group set-up and member enrollment time

Two outstanding problems
(many solutions exist, better ones may come along)

- Source authentication: How to verify integrity and authenticity of data when:
  - Only the source is trusted
  - Reliable delivery is not guaranteed
- Group membership management: How to maintain a common group key with dynamically changing membership.

Limiting the scope

- The group decided to concentrate on the following scenario:
  - Medium to large groups: 100K to 1M+ members
  - Single (or few) sources
  - Group Controller is trusted to generate and distribute keys
  - Members could impersonate sources
  - Illegal redistribution not addressed

Some basic design guidelines

- Separate security from data routing:
  - End-to-end security; no change in routing
  - No re-encryption en-route
- Separate key management from data handling
- Use existing algorithms whenever possible
- Minimize changes to OS kernel
- Maintain ability to plug-in different crypto algorithms