Secure Multicast:
A taxonomy

Ran Canetti
IBM Research

canetti@watson.ibm.com

Multicast group parameters

- Size
- Membership dynamics
- Life time
- Number of senders (known in advance?)
- Volume of traffic

Security requirements

- Access control
- Authentication:
  - Sender (individual, group)
  - Data
- Secrecy:
  - Long term (strong)
  - Ephemeral (weak)
- Anonymity:
  - From group members
  - From outsiders
- Availability

Trust issues

- Trust in a single center
- Trust in intermediaries

Levels of trust:

- To relay keys
- To generate keys
- To correctly encrypt/authenticate

Want to distribute trust!

Performance parameters

- Setup + enrollment time
- Membership revocation overhead
- Time to authenticate + encrypt data
  (at sender)
- Time to verify + decrypt
  (at receivers)
- Communication bandwidth overhead
- Length of keys

Benchmark scenario (I):

- Single (few) senders with strong machines
- Many recipients (100K — 1M+) with weak machines
- Dynamic, bursty membership
- Weak/ephemeral secrecy needed
- Strong authenticity needed

Examples:

- Pay-per-view movies
- News casts
- Stoc quotes
- ...

Benchmark scenario (II):

- Medium/small groups (100s — 10K-)
- Many senders (unknown in advance)
- Slowly changing membership
- Strong secrecy (sometimes)
- Strong authenticity

Examples:

- Video conferences
- Classes, lectures
- Town hall meetings
- Multiparty games

Existing solutions

Distributing a single key:
(Good for secrecy and "group authentication")

Very partial list:

[Ballardie 96]

[GKMP 97]

[Iolus 97]

[Wallner et. al. 97]

[MKMP 97]

[Canetti et. al. 98]

Existing solutions

Authentication of individual senders:
(Problematic. Only partially satisfactory solutions are known.)

- Signatures:
  - Sign every nth packet
  - Use stream signatures [Gennaro et. al. Crypto 97]
  - Use signatures with cheap verification
- Multiple MACs [Canetti et. al., 98]
  - More efficient for small/medium size groups
  - Secure only against limited-size coalitions
  - Work in progress...
- Other solutions ?