A Privacy Architecture for Lightweight Sessions

Van Jacobson
Steve McCanne
Sally Floyd

Lawrence Berkeley Laboratory
Berkeley, CA 94720

ARPA Network PI Meeting
Santa Fe, NM
September 26–28, 1994

- The MBone tools work very well for ‘public’ conferencing.

- Two years of large-scale use has demonstrated that they are simple, scalable and robust.

- We want to show that they work as well for ‘private’ conferencing.

‘Private’ implies that the audience is restricted.

There are two models for restriction:

- Control distribution topology (i.e., send via unicast).

- Encrypt data and control key distribution.

Only the 2nd choice works.

Distribution control doesn't work because:

- Internet is too easy to tap.
- Unicast doesn't scale.
- Exposes users to 'network crud' (IP addresses, firewalls, distribution topology, . . .)

Why so much resistance to encryption?

First, there's a widespread myth that encryption is expensive and requires special hardware.

This is false.

Even mediocre, portable C code does DES and Triple-DES in software at near wire speed:

	Encrypt rate (Mbit/sec.)	
Machine	**DES**	**3DES**
DEC Mips (5200)	3.5	1.9
Sun IPX	3.9	2.0
I486DX2	5.1	2.9
DEC Alpha (3400)	10.5	6.2
HP 735	10.7	5.8
Sun SS-20/50	11.9	6.3
SGI R4400	14.5	9.1

Put another way, decrypting a DES encrypted, 128kb/s video stream on a SS-20 can cost at most 1% of the processor.

(Of all the processing you have to do on multimedia data, encryption and decryption probably cost the least.)

However, while processing cost isn't a barrier to encryption, Government policy is:

Bizarre export regulations make it almost impossible for industry to commercialize products containing encryption.

But, since we can't solve this problem we ignore it and craft a solution for a totally hypothetical world where politicians behave rationally . . .

Basic design problem:

How to use encrypted multicast without putting too much burden on users?

Our model:

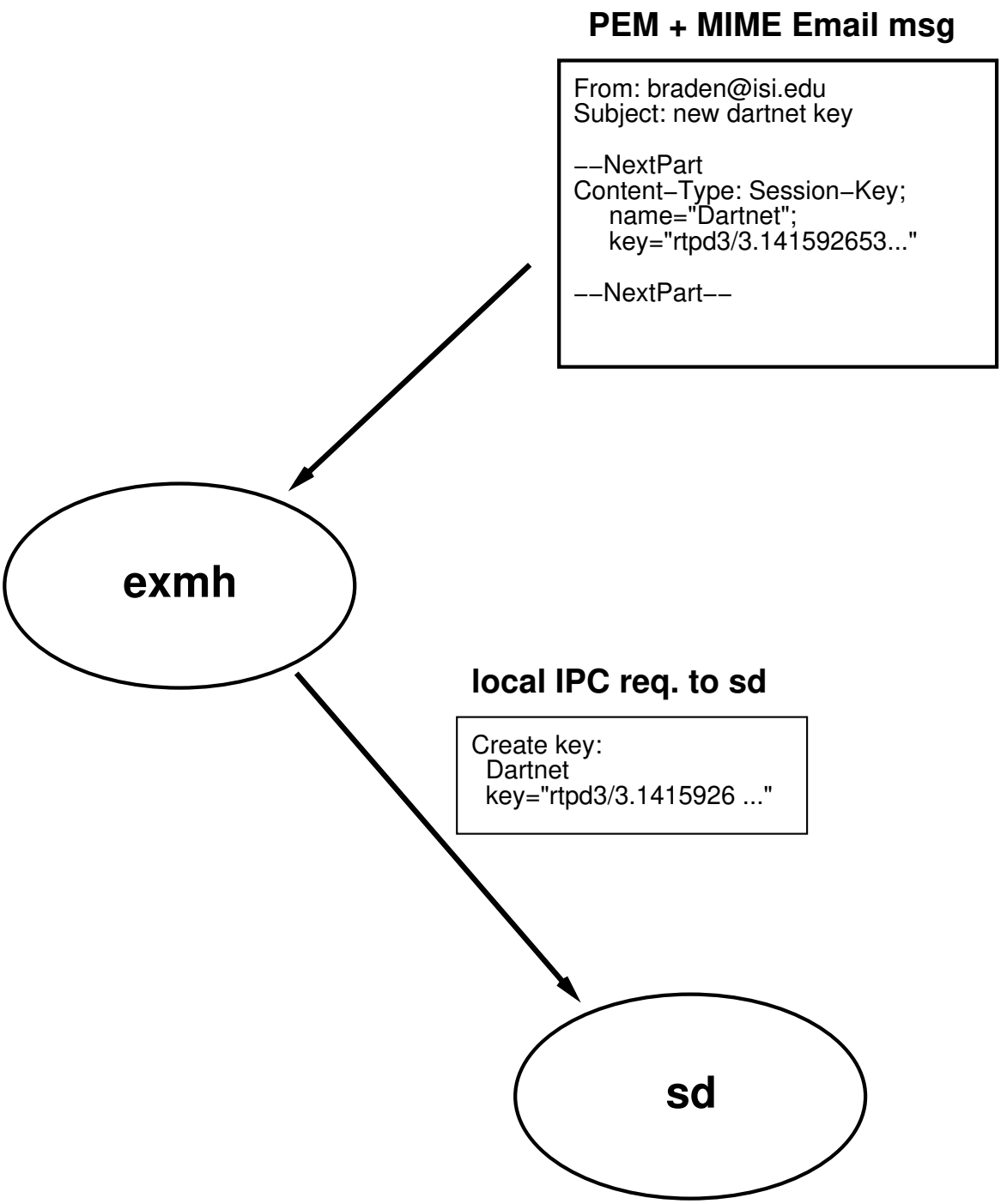
- User (or user's agent) can easily 'register' keys with sd.

- When session created, key can be specified to encrypt announcement packet.

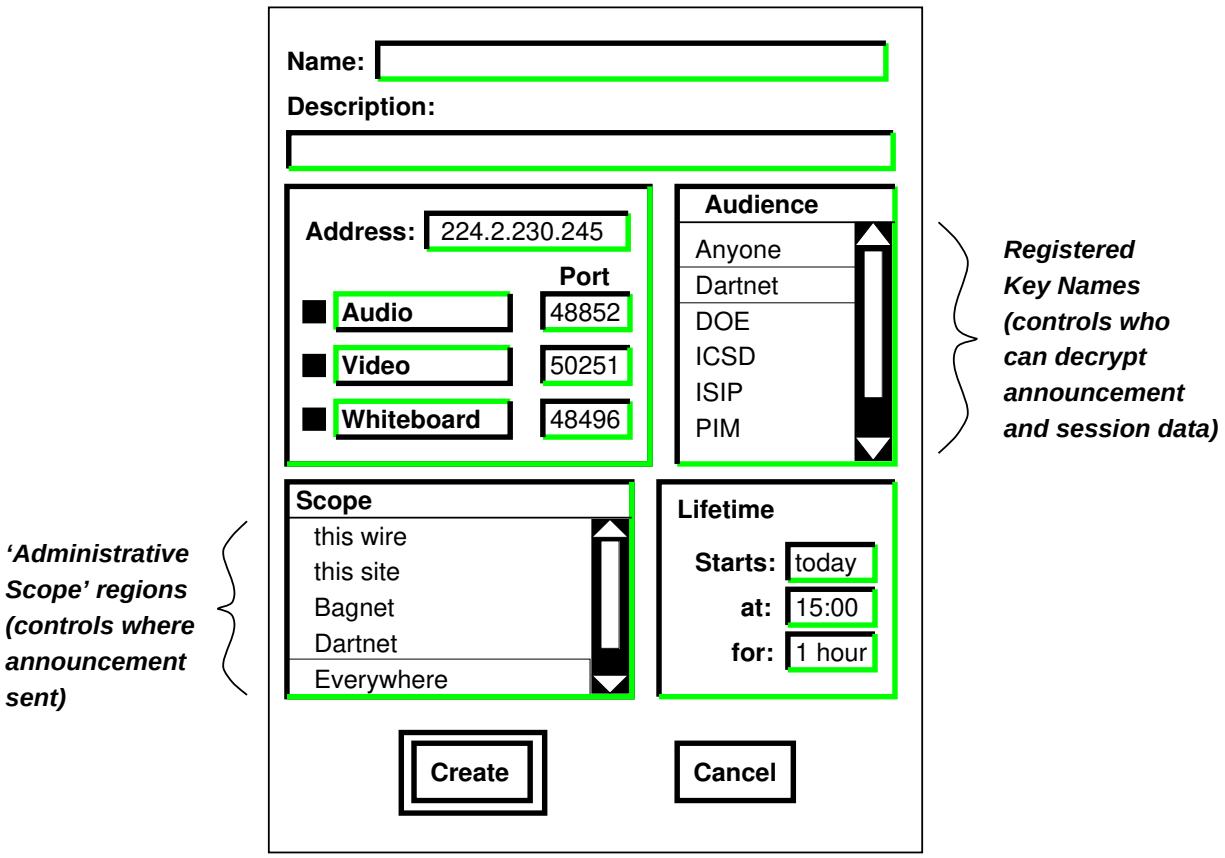
- When sd gets a malformed packet, it tries decrypt with all registered keys. If successful, announcement displayed & key is remembered.

- When session started, key handed to all tools of the session.

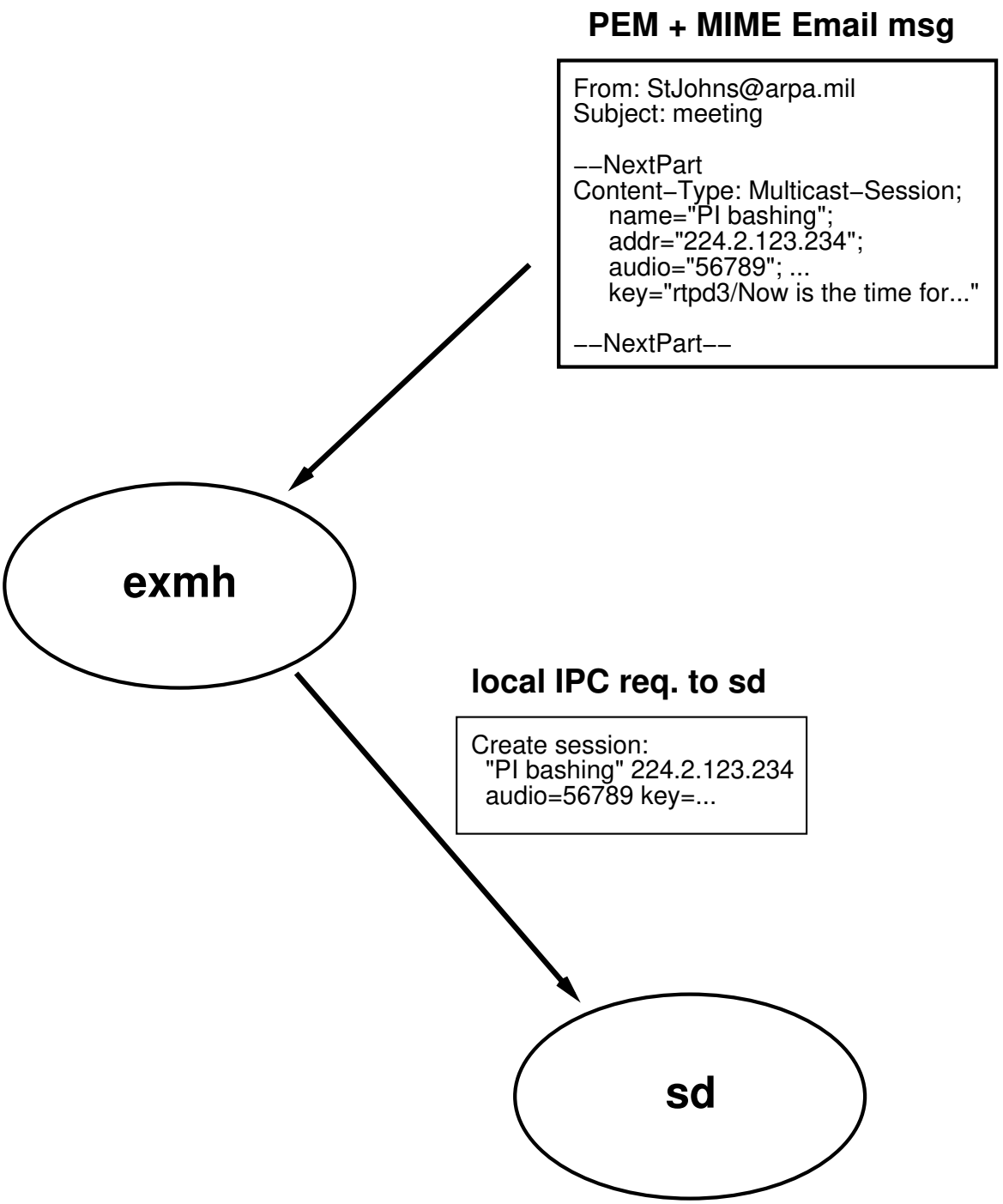
Sending a key to some closed group



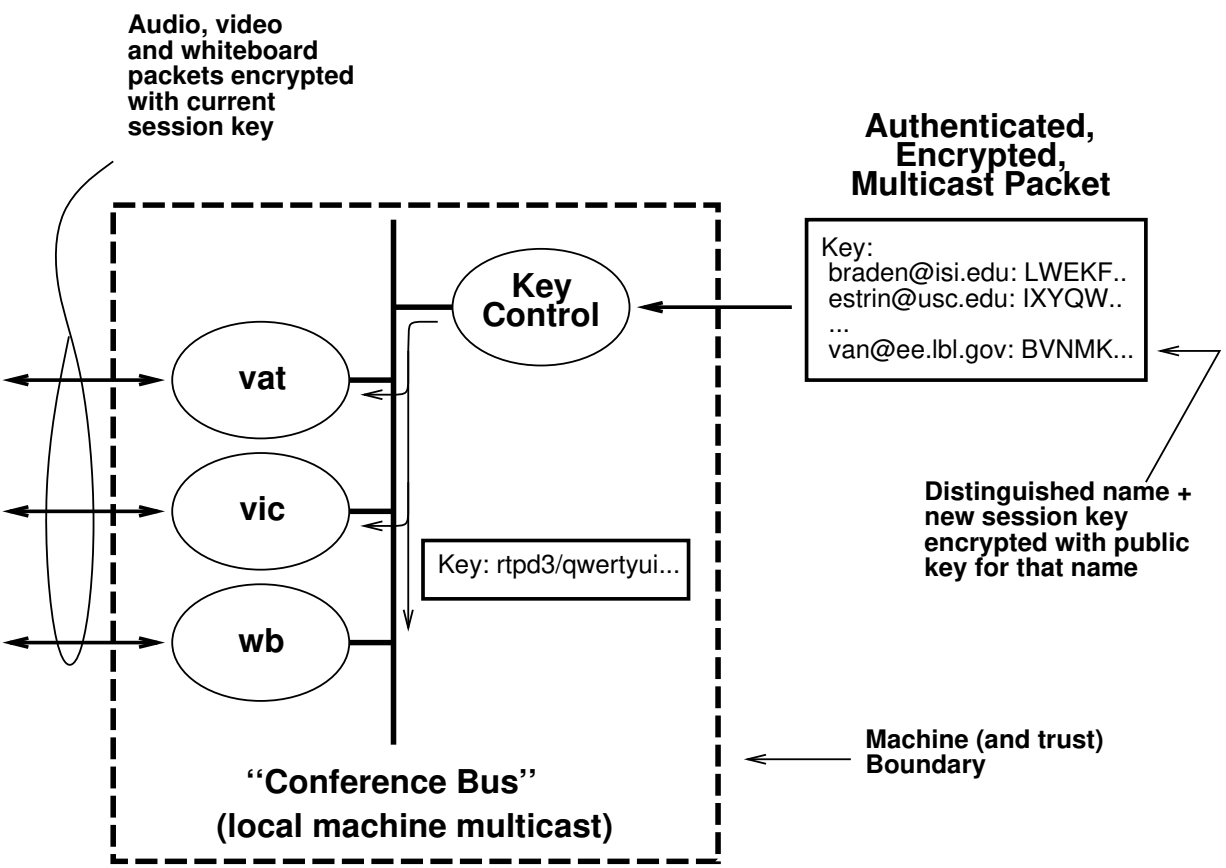
Changes to sd ‘new session’ dialog



Creating a private session via PEM



More sophisticated privacy models



Recap:

- Can create arbitrary ‘private’ groups by simply sending key to members of group.

- Any member of group can easily create session where announcement and data will be encrypted with group’s key.

- No new user burden for privacy: Session key for encrypted sessions automatically derived by sd (via search over registered keys).

Recap (cont.):

- Entire session announcement, including one-time, per-session key, can be communicated via external (non-multicast) means. E.g., Privacy-enhanced MIME message.

- Heavier-weight privacy models (dynamic re-key / key revokation, key schedules, external codebooks, etc.) can be implemented via ‘key control’ agents on “Conference Bus”. (Sd will automatically start key agent when it starts conference media tools).