How to get control over email?

Patrik Fältström

Internet Architecture Board

paf@cisco.com

Given a hammer, where are the nails?

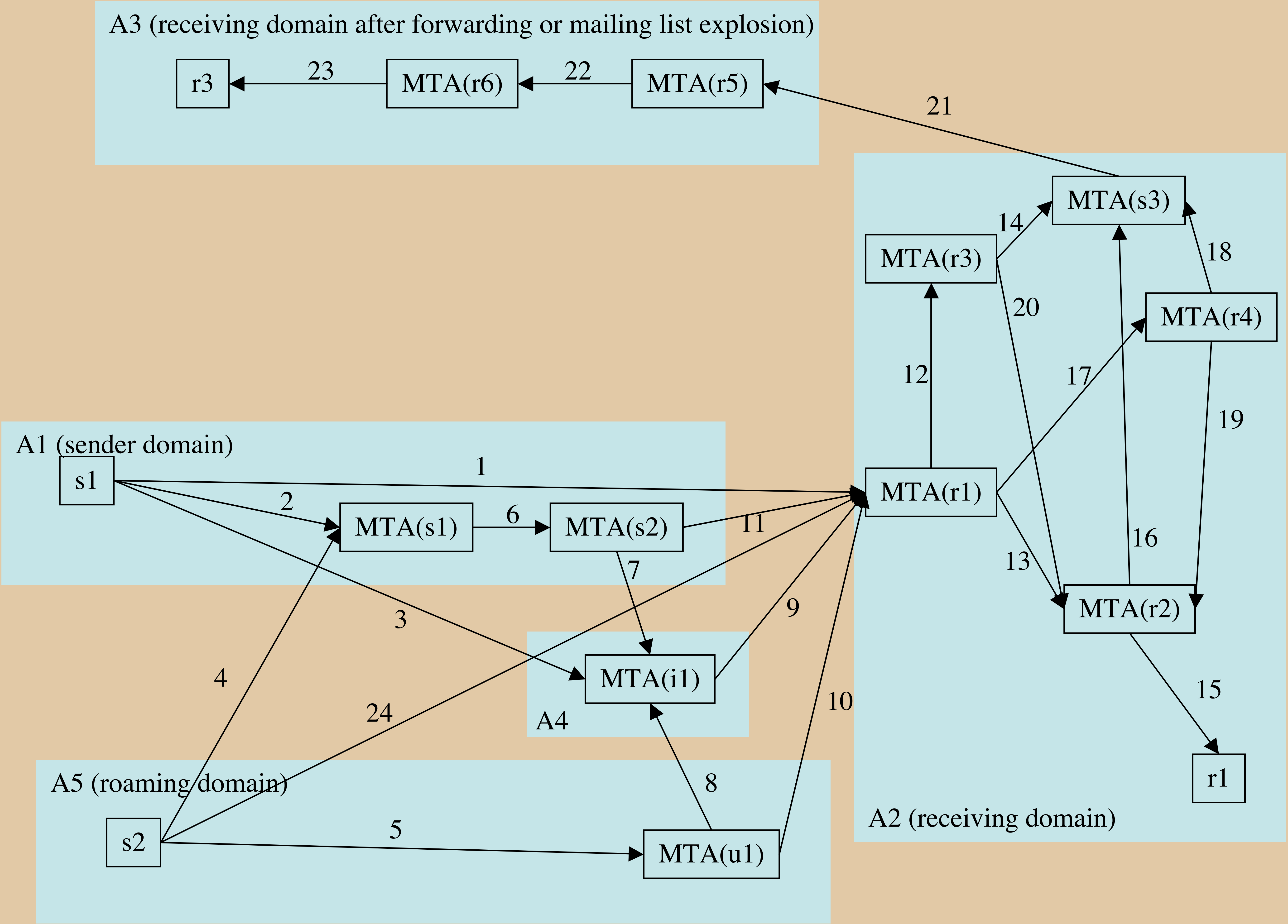
- My view is that people attack the spam problem from the wrong angle
  - Look for a solution
  - Fine-tune it
  - Look for a problem the solution solves

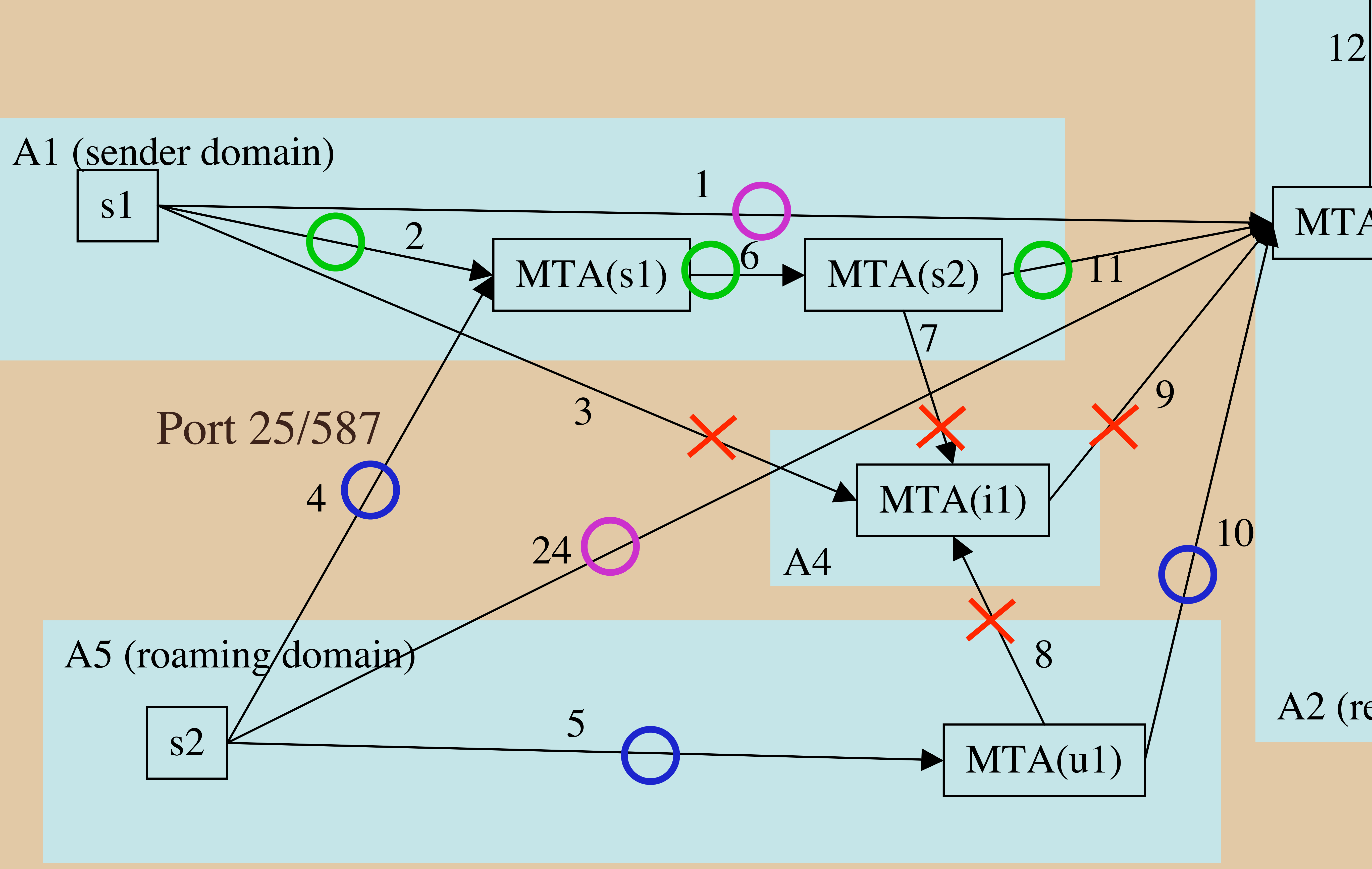
Alternative method

- Look at the problem
- Agree on what the problem is
- Find a solution to the problem

How is SMTP used?

- In many ways...
- Between many different entities...
- Spam, worms, trojans etc are injected in a “proper” mail flow...
- How, when where?


A3 (receiving domain after forwarding or mailing list explosion)
r3
23
MTA(r6)
22
MTA(r5)
21
MTA(s3)
14
MTA(r3)
18
20
MTA(r4)
12
17
19
A1 (sender domain)
s1
1
2
MTA(s1)
6
MTA(s2)
11
MTA(r1)
7
16
13
9
3
MTA(r2)
4
MTA(i1)
24
10
15
A4
r1
A5 (roaming domain)
8
A2 (receiving domain)
s2
5
MTA(u1)


12
A1 (sender domain)
s1
1
2
MTA(s1)
6
MTA(s2)
11
MTA
7
9
Port 25/587
3
4
24
MTA(i1)
A4
10
8
A5 (roaming domain)
s2
5
MTA(u1)
A2 (re

Technical solution?

- We can only do a limited number of things to "email" as we know it today
- One thing is "authentication of sender"
  - The IETF is looking into this now
  - It can minimize the number of false sender addresses
- Alternative is a new protocol

Two kind of proposals

- Signing mail (authenticate sender)
- “Reverse MX” and other (DNS) based

Followup issues

- Proposals will “just” make it possible to know who the mail comes from
- Proposals work on envelope sender, but many people working with anti-spam don’t know the difference, or want to secure header-from...
  - (which I see as a much harder problem due to mailing lists etc)

I think...

...we need:

- Technical methods to track violators
- Legislation
- Police (etc) which do the tracking

IETF (etc) only work with the 1st of these

Patrik Fältström

paf@cisco.com