Spam Is Bad

John R. Levine
Chair, IRTF ASRG
Chair@asrg.sp.am
http://asrg.sp.am
Why is spam bad?

- There’s too much of it
- It’s offensive
- It’s fraudulent
Why is spam bad?

- There’s too much of it
  - More spam than real mail everywhere
  - Large ISPs see > 80% spam
  - Even with filters, real mail is lost in the noise
Why is spam bad?

• *It’s offensive*
  – Large amounts of porn
  – Porn in the spam itself
  – Who’d give their kid an e-mail account?
Why is spam bad?

- It’s fraudulent
  - All those fake addresses
  - Forgeries of familiar addresses
  - Selling fraudulent stuff
  - Who’ll read real mail from the bank after getting 1000 fake mails from the bank?
What Isn’t the Spam Problem?

- The Authentication Problem
- The Introduction Problem
- The Filtering Problem
- The Accreditation Problem
- The Reputation Problem
The Authentication Problem

- Verify that a message is actually from the sender it purports to be from
The Authentication Problem

- Verify that a message is actually from the sender it purports to be from
The Authentication Problem

• Verify that a message is actually from the sender it purports to be from
• Same person as last time?
The Authentication Problem

- Verify that a message is actually from the sender it purports to be from
- Same person as last time?
- An actual real-life person?
The Authentication Problem

- Verify that a message is actually from the sender it purports to be from
- Same person as last time?
- An actual real-life person?
- An entity against which we can retaliate?
The Introduction Problem

- Mail from hitherto unknown senders
- Make it hard enough to deter spammers
- But easy enough to admit real mail
The Introduction Problem

- Mail from hitherto unknown senders
- Make it hard enough to deter spammers
- But easy enough to admit real mail

  E-postage    Hashcash

  CAPTCHA     Challenge/Response
The Filtering Problem

- Distinguish nice mail from nasty mail
- Try not to lose too much nice mail
- Hope it’s not too expensive to do
- Hope my tastes and yours aren’t too different
The Accreditation Problem

• Third parties that vouch for potential correspondents
• You can prove you’re nice to one place rather than millions?
The Accreditation Problem

• Third parties that vouch for potential correspondents
• You can prove you’re nice to one place rather than millions?
  – Bonded Sender
  – Habeas
  – IADB (ISIPP Accreditation Database)
The Reputation Problem

- Who’s nasty, who’s nice
- State of the art: DNSBLs
- Needs a lot of work
  - What do you ask a reputation system?
  - What kinds of answers can they return
Are These the Spam Problem?

• NO
• They’re related to it
• But they’re not the spam problem
• Or even necessarily parts of it
What has ASRG done lately?

• Reorganized into subgroups
• One finished, a few under way
Lightweight MTA Authentication Protocol

- Threw it over the wall to MARID
- Reborn as SMTP authorization
  - Looking at analysis of effect of whatever MARID does
Abuse reporting

- Simple convention for exchanging spam reports as e-mail
- Large ISPs express interest
• Drafted a few
  – DNSBLs / DNSWLs
  – Port 25 blocking and SUBMIT
Filtering

- Some work on a header to document what filtering has happened
- Now looking at filtering rule exchange
Message verification

- Domain keys, Authenticated Mail, TEOS, Lumos, S/MIME, ...
- Look for common aspects
  - Probably redundant with MASS
Identity, Authentication, and Reputation

• Lots of interest, no action
• Sender-ID et al need a reputation system
• How do we build them? What are the questions? What are the answers?
• Can we invent common interfaces?
Things we’re not doing

• Define spam
• Challenge/response
• E-postage
• Replacements for SMTP
What’s happening elsewhere

- Open Group
  - Validation profiles
- MAAWG
  - Implementation advice to members
- ITU-T
  - Technical and administrative coordination
  - Tell governments what to endorse
## The standards process

<table>
<thead>
<tr>
<th>IETF</th>
<th>ITU-T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practical orientation</td>
<td>Driven by politics</td>
</tr>
<tr>
<td>Based on working prototypes</td>
<td>Paper designs</td>
</tr>
<tr>
<td>Fast efficient process</td>
<td>Slow cumbersome process</td>
</tr>
</tbody>
</table>
The standards process

ITU-T
- Practical orientation
- Based on working prototypes
- Fast efficient process

IETF
- Driven by politics
- Paper designs
- Slow cumbersome process
So where are we?

- Spam is still bad
- Solutions are hard
- But we can make incremental progress
Spam Is Bad

John R. Levine
Chair, IRTF ASRG
Chair@asrg.sp.am