DISPATCH stuff – IETF113 Vienna

Bron Gondwana
<brong@fastmailteam.com>

Some things to talk about

- Rcpt-To: → avoiding DKIM replay attacks
- ARC supported here → recipient DNS record
- The large file via email problem

DKIM Replay

- Send a single spam email to somebody via a trusted provider, it gets DKIM headers that verify.
  - Blast that email via any sending IP to millions of people, using envelope “RCPT TO” without changing the “To:” header.
  - It passes DKIM!
- This is big **right now**. Was a major topic at M3AAWG.

DKIM Replay Protection

- Option: add a “Rcpt-To:” header which must align with the envelope:
  - Can’t send to multiple recipients in a single SMTP session.
  - Nobody does this anyway. VERP, etc.
- Breaks ALL indirect mail flow
  - Right now you can forward without breaking DKIM

DKIM Replay

- Any other suggestions?
- Need to solve the indirect mail flow issue.
  - ARC!

“ARC accepted here”

- ARC has a bootstrap problem:
  - If sender has a DMARC policy, forwarder must rewrite sender
  - UNLESS forwarder knows that recipient will accept ARC
- ARC signal must come from recipient, not sender.
  - Solution: add “ARC supported” signal to the recipient.

ARC accepted signal

- Add to SMTP capabilities?
  - MX could reply “I accept ARC” to EHLO.
  - very late for sender to have to update message on the fly while connected.
- Add to DNS?
  - Lookup a record on recipient domain
  - or a record for each MX
- Need to know for each hop, only if all support can you avoid rewriting
- Do we also need a way for a sender to say “I don’t accept being forwarded”?

The large file problem

- Discussed at last DISPATCH
  - Alexey and I are working on speccing it out
  - Content-Digest: header → work also happening in HTTPBIS that we can build on
  - Planning to do some experiments before next IETF, building on message/external-body from RFC2046
- Let us know if you’re interested in working on it.