Malformed Message Handling BCP

Murray S. Kucherawy

<msk@cloudmark.com>

History

- For various reasons, mostly to keep support costs down and invite participation, email components are historically lax at enforcing standards like RFC5322
- Recently this has become a security issue, where different parts of the mail system treat various malformations in their own ways

History

- That means a particular malformation might be handled one way at a border MTA or filter, and then another way at the MUA
  - Prime example: A message with two From: fields; border MTA/filter acts based on the “bottom” (first one), while MUA shows the “top” (second one)
  - Another example: Malformed lines in the header block, where some components switch to “body” mode and others don’t
- This can be exploited in phishing attacks, spam, etc.

Goals of this work

1. Strongly encourage MSAs to be a lot more strict in what they allow into the mail stream, specifically because of the exposure created by not doing so
2. Highlight common malformations and provide advice about what to do with them (interpretation, handling, correction, etc.) based on experience and consensus of the community

Not the goals of this work

- Loosen the standards to allow common malformations because they are common in reality
- Elevate any malformation to have any kind of real or perceived “standard” status

Current draft

- draft-kucherawy-mta-malformed-bcp
  - Contains the initial idea; more cases can and should be added by the community
- Needs a home
  - A wiki?
    - But the IESG didn’t like that idea much
  - APPSAWG?
    - Concern that the advice in the BCP will change over time as the problems evolve
    - …but RFCs can be updated as necessary
  - Individual submission?

Discussion

- <your ad here>