SMTP Greylisting BCP

Murray S. Kucherawy
<msk@cloudmark.com>

What’s Greylisting?

- A fairly common practice in the email world wherein an SMTP server temp-fails traffic from a source it’s never seen before
- Assumption is that legitimate mail servers will queue and retry, while spammers’ bots won’t bother
  - On retry, the message will generally succeed
- So it’s not a protocol, but rather a heuristic that takes advantage of a property of compliant implementations

Pros

- End users don’t need to do anything to get their mail through a greylisting filter when it transits compliant MTAs
- Doesn’t take much for administrators to set up
- Reduces load on content scanning spam filters
  - Which are much more compute-intensive

Cons

- The original idea that two people can exchange email, generally with immediate results, is no longer true
- Requires storage to remember which triplets (IP address, sender, recipient) it has seen before
  - This is a big deal at scale
- Some very old clients and MTAs treat 4yz errors as permanent failures
- Can cause a warning DSN, which upsets users
- If the retry comes from another IP address, additional delays are introduced

Why do we care?

- The practice has been around for a long time
  - Seminal white paper written by Evan Harris in 2003
- We’re discovering that lots of people have different understandings of what the term means and how the process works
  - Some people at MAAWG thought any 4yz reply is greylisting
- Also discovering that not everyone is aware of all the “cons”
- It’s high time someone wrote all this down

What about that other thing?

- Also an effort afoot to create an SMTP extension for relaying policy information on a temporary failure
  - For example, being able to tell the client "Not now, try again in 30 minutes" when greylisting would avoid retries that are guaranteed not to work
  - Similar in the load shedding scenario
- This is *not* that

So now what?

- draft-kucherawy-greylisting-bcp is an outline for a document to do just that
  - Enumerates pros and cons
  - Discusses implementation variants
  - Recommends implementations and parameters for specific example scenarios
- YAM has terminated, so there's no WG specific to email right now that could pick this up
- Suggest APPSAWG is the right place to process this