DMARC WG
Online Bangkok 2020

Chairs:
Alexey Melnikov <alexey.melnikov@isode.com>
Seth Blank <seth@valimail.com>
Tim Wicinski <tjw.ietf@gmail.com>

Note Well

- This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

- As a reminder:

    - By participating in the IETF, you agree to follow IETF processes and policies.

    - If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.

    - As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.

    - Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

    - As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Note Well
(continued)

- Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:
  - BCP 9 (Internet Standards Process)
  - BCP 25 (Working Group processes)
  - BCP 25 (Anti-Harassment Procedures)
  - BCP 54 (Code of Conduct)
  - BCP 78 (Copyright)
  - BCP 79 (Patents, Participation)
  - https://www.ietf.org/privacy-policy/ (Privacy Policy)

Administrivia

- This Meetecho session is being recorded
- Meetecho:
  - https://meetings.conf.meetecho.com/ietf109/?group=dmarc&short=&item=1
- Jabber room (discussions/back channel):
  - dmarc@jabber.ietf.org
- Shared note taking:
  - https://codimd.ietf.org/notes-ietf-109-dmarc
- Note taker?

Agenda

- Agenda bashing, administrivia, note well (chairs) - 5 **mins**
- **Should we deprecate** “pct” tag?
- Aggregate reporting
    - ARC reporting
    - extensible reporting
    - NXDOMAIN reporting
- Failure reporting
- Break out definition of org domain to a different document?
- Policy discovery: tree walk?

WG Status

- DMARCbis draft was split into 3 parts: base spec, aggregate reporting, failure reporting.

draft-ietf-dmarc-dmarcbis-00
Should we deprecate the **pct** tag?

pct: (plain-text integer between 0 and 100, inclusive; OPTIONAL; default is 100). **Percentage of messages from the Domain Owner's mail stream** to which the DMARC policy is to be applied. However, this MUST NOT be applied to the DMARC-generated reports, all of which must be sent and received unhindered. The purpose of the "pct" tag is to allow Domain Owners to enact a slow rollout enforcement of the DMARC mechanism. The prospect of "all or nothing" is recognized as preventing many organizations from experimenting with strong authentication-based mechanisms. See Section 6.6.4 for details.

draft-ietf-dmarc-dmarcbis-00
Should we deprecate the **pct** tag?

- What is the problem?
  - Written, implemented, and understood differently
  - cause of lots of shenanigans
  - more damaging that it's worth?

- Written: applied to percentage of all mail
  - This is bad math, as mail is not a uniform sample

- Understood: applied to percentage of failing mail

- Implemented:
  - Some gateways treat pct=[anything] as pct=100
  - p=reject; pct=75% results in 90% quarantine

- Perverse incentives:
  - p=quarantine; pct=0

draft-ietf-dmarc-dmarcbis-00
Should we deprecate the **pct tag?**

- Is it needed, when we already have “p=quarantine”?
- Or do we want to clarify definition to make consistent implementation easier?

- DISCUSS

draft-ietf-dmarc-aggregate-reporting-00

- Extensible reporting
  - What kind of extensions should be allowed?
  - What's needed for future authentication mechanisms to be folded into DMARC?
  - Extending reports for arbitrary authentication mechanisms to be reported makes it easy to collect data and run experiments without modifying the spec

draft-ietf-dmarc-aggregate-reporting-00

- ARC reporting
  - Fold text from RFC 8617, Section 7.2.2
  - Add structured fields so ARC data is more parseable hop to hop
    - A text comment field isn't good enough, given the amount of data

- NXDOMAIN reporting

  Ticket #60: Public Suffix Domains might want a special type of reporting limited to NXDOMAINs being used to send email within their zones. One of the key uses cases being discussed as part of PSD is not just blocking unauthenticated being sent from NXDOMAINs, but being able to gather some data on what exactly is being abused. An NXDOMAIN aggregate report meets this need, and is desirable for operators PSDs.

  Data has been shared with the list that mail is being sent and *delivered* from NXDOMAINs of PSDs that wish for this functionality.

draft-ietf-dmarc-failure-reporting-00

- Slimmed down reports with minimal PII
  - What should and should not be included?
  - Straw man was just From and To
  - Is this a failure report sent as failures occur, or could this be sent at a regular interval like an aggregate report?

Break out definition of org domain to a different document?

- DMARC is cluttered by the definition of Org Domain, and the rest of the mechanism is separate
  - There appears to be some desire in the group to break this definition out to a) simplify the base spec, and b) provide an inheritable definition of Org Domain that can be used for other mechanisms
- Pros? Cons?
- Editor?

Policy discovery

- DNS tree walk?
- DNS tree walk!

- A host of use cases aren't suited by DMARC's current policy discovery mechanism
  - Orgs within orgs (think governments, universities)
  - TLDs (explicitly prohibited per mechanism)
- All these simplify into a single use case if we just walk the tree until we find a DMARC record
  - But will need protections to limit abuse of malicious labels