DMARC: Domain-based Message Authentication, Reporting and Conformance

Tim Draegen
<tim@eudaemon.net>
The Problem With Email

Email Abuse

- Email is consistently a factor in online abuse.
- Determining authenticity of email is difficult.
- Email is ubiquitous – *changing it is really hard.*

DMARC.ORG

- Coalition of ~17 companies/organizations.
- Goal to reduce abuse by solving several long-standing issues related to email authentication protocols.
- Draft specification, resources, FAQ, mailing list all on [DMARC.ORG](http://DMARC.ORG)
- Building on existing tech (SPF and DKIM) whenever possible, only inventing when necessary, informed by in-production experience.
Lessons Learned from SPF & DKIM

- No consistency to how DKIM and SPF are deployed.
  - Receivers used whatever was deployed/available.
  - Senders tried hard to check the box.

- Receivers couldn’t rely on accuracy of Sender’s auth.
  - As rule, Senders failed to cover all email, significantly reducing utility.

- Senders had no visibility into email domains usage.
  - Impossible to discover usage through auditing process.

- ROI for “email authentication” didn’t add up.
What DMARC Brings

- **Overlay** – SPF and DKIM used as authentication mechanisms:
  - Header-From: domain used to link SPF and DKIM to email
  - Consistency on how to deploy SPF and DKIM
- **Feedback** – Domain owners get access to what Receivers see:
  - Domain owners can quickly/accurately cover legit email w/ auth.
- **Policy** – Domain owners declare how to process failing email:
  - Specifies DNS-based model that incorporates SPF + DKIM results

### SPF

- *Path-based* (RFC 4408)
- Authorized servers published via simple DNS record
- Very low deployment cost
- Forwarding breaks SPF

*Is the messenger (server) permitted?*

### DKIM

- *Signature-based* (RFC 6376)
- Requires cryptographic operation by email gateways
- Public keys published via DNS
- Can survive forwarding

*Is the signature authentic?*
DMARC meets “Lessons Learned”

• No Consistency to how DKIM and SPF are deployed.
  ▫ Receivers used whatever was deployed/available.
  ▫ Senders tried hard to check the box.

• Receivers can rely on accuracy of Sender’s auth.
  ▫ As rule, Senders failed to cover all email, significantly reducing utility.

• Senders have no visibility into email domains usage.
  ▫ Possible to discover usage through auditing process.

• ROI for “email authentication” adds up.
DMARC Today & Future

- Works today:
  - E.g.: One participant sees ~600,000,000 rejected abusive emails annually due to DMARC-based controls.

- In the Future:
  - DMARC.ORG goal is to submit draft specification to IETF so that it may begin the process of becoming an official Internet Standard RFC – available to everyone for reference, implementation, and improvement.

- All Info @ DMARC.ORG