DMARC and related standards

Sam Silberman, Constant Contact

Topics

- DMARC Retrospective
- Security/Privacy
  - TLS over SMTP
  - End-to-end encryption
- SMTP over IPv6
- Activities in the IETF APPSAWG

How does DMARC work?

- Organization publishes a DMARC policy on their domain
  - P=none
- Participating ISPs sends the organization authentication and forensic reports
- Organization audits their outbound sending practices
  - Centralizes outbound mail
  - DKIM signs all outbound mail
  - Publishes/updates SPF
  - Repeat
- Only after exhaustive analysis, organization can enable DMARC p=reject

Who should enable DMARC?

- Large organizations who's brand (domain name) is used as part of a phishing scam.
  - Banks (BOA, Amex)
  - Popular brands (PayPal, Ebay, Amazon)
  - Government agencies (IRS)

Who should not use DMARC?

- Any organization where the mailbox owner demands the option to enable/disable the DMARC policy
  - Mailbox service providers (ISPs)
  - Large corporations (no brand risk)
- When individuals within the org need to send mail via relays
  - Mailing lists
  - ESPs

The ESP experience of p=reject

Our Customers

Two types of customers

- Switched their email FROM address to use a hosted domain
- Switched their email FROM to use different mailbox provider
- Did nothing

Proposed Mitigations

- Customer use non-DMARC hosted mailbox
- Proxy FROM address (Address re-write)
  - FROM "Sam" sam+yahoo.com@ccsend.net
  - Reply-To: sam@yahoo.com
- Obtain permission to DKIM sign on behalf of ISP
  - AOL.COM CS.COM AIM.COM
- Relay through domain owner's SMTP server
- Other ideas posted on the ASRG site

http://wiki.asrg.sp.am/wiki/Mitigating_DMARC_damage_to_third_party_mail

Security/Privacy

- TLS over SMTP
  - SMTP security via opportunistic DANE TLS
    - http://tools.ietf.org/html/draft-ietf-dane-smtp-with-dane-12
- End-to-end encryption
  - Google's proposal
    - JavaScript-based crypto library.
    - OpenPGP standard
  - IETF discussions "Endymail"

SMTP over IPv6

- **SMTP IPv6 to IPv4 Fallback**
  - http://tools.ietf.org/html/draft-martin-smtp-ipv6-to-ipv4-fallback-01
- Required authentication (best practice)
  - Linkedin position
    - https://engineering.linkedin.com/email/sending-and-receiving-emails-over-ipv6
  - Google's position
    - https://support.google.com/mail/answer/81126?p=ipv6_authentication_error&rd=1#authentication

Activities in the IETF APPSAWG

- NULL Mx
  - http://datatracker.ietf.org/doc/draft-ietf-appsawg-nullmx/
- A Property Types Registry for the Authentication-Results Header Field
  - http://datatracker.ietf.org/doc/draft-ietf-appsawg-authres-ptypes-registry/
- The Require-Recipient-Valid-Since Header Field and SMTP Service Extension
  - http://datatracker.ietf.org/doc/rfc7293/
- Advice for Safe Handling of Malformed Messages
  - http://datatracker.ietf.org/doc/rfc7103/
- Deprecating the "X-" Prefix and Similar Constructs in Application Protocols
  - http://datatracker.ietf.org/doc/rfc6648/

Questions?

Sam Silberman: ssilberman@constantcontact.com
@samuelsilberman