Using DMARC

DMARC is new kind of “policy publishing”

Early stages of gaining experience with deployment and use

- *Let's help folks*

Rough draft BCP ⇨ `draft-crocker-dmarc-bcp`

- *Guide new adopters*
- *Raise issues amongst current operators*

Overview 2-3

2. Development
{T. Draegen}

Developing Components

Developing Compliant Systems

Sending Compliant Email

≈

(DKIM/SPF) + DMARC/TXT

From: field alignment

Organizational domain

SMTP-time vs. later

3. Barriers to Adoption (Fears)
{A. Popowycz}

Where is all my email is sent from?

Will I lose flexibility in email delivery?

Use of 3rd-party senders requires complex coordination?

Auto-forwarded mail often breaks DMARC (like mailing list problem)

Overview 4-5

4. Planning for DMARC adoption {E. Zwicky}

Integration and use:

- *Decide what you need to do - p=quarantine & p=reject not intended for all use cases*
- *Picking alignment and SP parameter values - tight for single domains; loose for many*
- *Incremental roll-out, Sending - start w/easiest and/or most attacked*
- *Incremental roll-out, Receiving - handling action vs. reporting*

5. DNS Configuration {M. Hammer}

- *Malformed Policies*
- *Reporting malformed policies back to owner (RUA) or Whois contact*
- *Managing records - automate DKIM key rotation & DMARC records*
- *Publishing reject policies for non mailing domains(!)*

Overview 6-7

6. Receiver Processing {S.Solanki}

Preparing for processing - looks at patterns of incoming domain names, abuse msgs, etc.; scoping implementation

Implementing at receiver - DNS performance, DMARC caching, reporting schedule, instrumentation, confg tweaking, {user display of trust?}

Rolling out - coordinate w/trusted senders, apply incrementally

*Post roll-out - monitor! / **give feedback to DMARC community!***

7. Report Generation {M. Jones}

Detailed guidance, caveats, reminders, examples:

Aggregate report naming and metadata - compressed & uncompressed have same name; guidance on fields

Minimum requirements for aggregate report records

Use and reporting of local policy "overrides" - receiver not "required" to comply

Minimum requirements for failure reports - failure of legitimate mail; occurrence of abuse

Overview 8

8. Report Receipt and Analysis
{M. Jones}

Report Receipt - typically daily email; typically few mail receivers

Report Analysis - correlate IP Addrs, reported volume, authentication failures; check for "new" mail sources(!),

Report Processing & Analysis Svcs - specialists are emerging...