DMARC
Providing domain owners control of their brand in the email channel

January 2012
DMARC Defined

DMARC stands for:

Domain-based Message Authentication, Reporting & Conformance

(pronounced “dee-mark”)
DMARC.org is Formed

A loose collaboration of leading organizations working for 18 months to develop an Internet standard that enables senders and receivers to communicate email authentication information to thwart phishing.
Phishing continues to be a major pain point for the consumer Internet.

- 90% peak spoof rates
- 10% average spoof rate of the Internet Retail 500
- 30% average spoof rate for top federal government sites

Incidence and costs related to spear phishing rising quickly:
- 100k's account hijackings daily

Loss of trust in online resources
Decrease in future online activity

1 Source: Online Trust Alliance https://otalliance.org
SPF and DKIM adoption reaching the tipping point

Majority of clean mail is authenticated

1Courtesy, DMARC.org member company
The Challenge for Senders
Mail Authentication is hard and with uncertain ROI

- SPF: IPs
- DKIM: Pub Keys
- Keystore: Private Keys
- DNS: SPF and DKIM

Salesforce
SaaS Tool

Enterprise boundary

Receivers

Spammers and Phishers

© 2012 DMARC.org
The Challenge for Receivers
Senders adding some authentication helps only a little

If the sender isn't signing all their messages, we still are forced to guess what's phishing and what's not.
The Solution
Senders authenticate ALL mail and tell that to receivers

If the sender is signing all their messages, the receiver knows unsigned messages are phishing.
DMARC Identifier Alignment

- DMARC combats phishing by tying Mail User Agent (MUA) visible "RFC5322.From" field to the DKIM or SPF authenticated domain
- Identifier alignment can be strict (match exactly) or relaxed:
  - Relaxed SPF: SPF Authenticated RFC5321:Mail From and RFC5322:From must share Organizational domain
  - Relaxed DKIM: Organizational domain from 'd=' value of DKIM authenticated signature must be equal or parent to RFC5322:From
DMARC from Author to Recipient

1. **Author Composes & Sends Email**
2. **Sending Mail Server Inserts DKIM Header**
3. **Email Sent to Receiver**

**SENDER**

- Validate and Apply Sender DMARC Policy
  - Retrieve Verified DKIM Domains
  - Retrieve "Envelope From" via SPF
  - Apply Appropriate DMARC Policy

**RECEIVER**

- Standard Validation Tests
- IP Blocklists, Reputation, Rate Limits, etc.
- Anti-Spam Filters, etc.

**Standard Processing**

- Passed
- Quarantine

**Update the periodic Aggregate Report to be sent to Sender**

**Failure Report sent to Sender**
DMARC Defines:

- **DKIM & SPF Configuration Guidelines**
  - Designed to achieve identifier alignment

- **DNS Resource Record**
  - A new TXT RR of sender policies including:
    - alignment types: **Strict | Relaxed**
    - disposition: **Quarantine | Reject | Monitor**
    - reporting URIs: **Failure & Aggregate**

- **Aggregate Reporting Format**
  - Aggregate of email disposition data over time.
  - XML syntax format for aggregate reports
DMARC DNS Record Options

- Domain owners post policies in the DNS, just like with SPF or ADSP
- Policy record consists of a series of DKIM-style “tag=value” pairs

<table>
<thead>
<tr>
<th>Tag Name</th>
<th>Purpose</th>
<th>Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td>Protocol version</td>
<td>v=DMARC1</td>
</tr>
<tr>
<td>pct</td>
<td>% of messages subjected to filtering</td>
<td>pct=20</td>
</tr>
<tr>
<td>ruf</td>
<td>Reporting URI for forensic reports</td>
<td>ruf=<a href="mailto:authfail@example.com">authfail@example.com</a></td>
</tr>
<tr>
<td>rua</td>
<td>Reporting URI of aggregate reports</td>
<td>rua=<a href="mailto:aggrep@example.com">aggrep@example.com</a></td>
</tr>
<tr>
<td>p</td>
<td>Policy for organizational domain</td>
<td>p=quarantine</td>
</tr>
<tr>
<td>sp</td>
<td>Policy for subdomains of the OD</td>
<td>sp=reject</td>
</tr>
<tr>
<td>adkim</td>
<td>Alignment mode for DKIM</td>
<td>adkim=strict</td>
</tr>
<tr>
<td>aspf</td>
<td>Alignment mode for SPF</td>
<td>aspf=relaxed</td>
</tr>
</tbody>
</table>
DMARC Reporting Specification

• Reporting is redacted for privacy
• Daily Aggregate reports, per From: domain
  o Does NOT contain delivery disposition
  o Does NOT contain individual email addresses
• Aggregate statistics by IP address
  o Authentication results for DKIM and SPF
  o DMARC identifier alignment results
  o Policy actions requested and taken

```
<record>
  <row source_ip="173.0.84.226" count="1963" policy_domain="paypal.com" policy="reject" action_taken="none" />
  <identities envelope_from="intl.paypal.com" header_from="intl.paypal.com" />
  <auth_results>
    <dkim result="pass" human_result="" d="intl.paypal.com" />
    <spf domain="intl.paypal.com" identity="spf_envelope_from" result="pass" />
  </auth_results>
</record>
```
Swimlane: **Sender to Receiver**

- **Sender** sends an email to **Receiver**.
- **Receiver** requests Sender's DNS records.
- **Receiver** responds with SPF RR, DKIM RR, and DMARC RR.
- **Receiver** checks DKIM & SPF and applies DMARC policy.
- If the email does not pass DMARC, a failure report is sent to **Sender**.
- **Receiver** adds disposition for inclusion in aggregate DMARC report.
- Periodic aggregate report sent to **Sender**.

© 2012 DMARC.org
DMARC Steps for Outbound Authentication

1. Deploy DKIM & SPF
2. Ensure identifier alignment
3. Publish a “monitor” record and ask for data reports (you will need the capability to process this data… build or buy)
4. Learn from the data, gain confidence in your mail streams
5. Slow roll actionable policies, from "monitor" to “quarantine” to “reject”
The Value of DMARC

Senders
• Improves resiliency of email authentication infrastructure
• Provides control over brand in email channel
• Lowers risk of hijacking
• Enables new forms of communication over email

Receivers
• Decreases spam
• Lowers risk of hijacking
• Enables new forms of communications over email
DMARC
Domain-based Message Authentication, Reporting & Conformance

Read the specification, and join the discussion at dmarc.org