M³AAWG DMARC Training Series

Mike Adkins, Paul Midgen
DMARC.org
October 22, 2012
M³AAWG DMARC Training Videos
(2.5 hours of training)

This is Segment 4 of 6
The complete series of DMARC training videos is available at:
https://www.m3aawg.org/activities/maawg-training-series-videos

<table>
<thead>
<tr>
<th>Segment 1</th>
<th>Segment 2</th>
<th>Segment 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is DMARC?</td>
<td>DMARC Identifier</td>
<td>DMARC Policy Records</td>
</tr>
<tr>
<td>(about 20 minutes)</td>
<td>Alignment</td>
<td>(about 30 minutes)</td>
</tr>
<tr>
<td>Segment 4</td>
<td>Segment 5</td>
<td>Segment 6</td>
</tr>
<tr>
<td>DMARC Reporting</td>
<td>DMARC Information</td>
<td>DMARC Information for</td>
</tr>
<tr>
<td>(about 15 minutes)</td>
<td>for</td>
<td>Domain Owners and 3rd</td>
</tr>
<tr>
<td></td>
<td>Mailbox Providers</td>
<td>Parties</td>
</tr>
<tr>
<td></td>
<td>(about 20 minutes)</td>
<td>(about 40 minutes)</td>
</tr>
</tbody>
</table>
DMARC Reporting
DMARC Segment 4 – about 15 minutes

Paul Midgen, DMARC.org
October 22, 2012
DMARC Spec – Reporting

Aggregate Reports

- Each report covers one RFC5322.From domain.
- You should get one from each supporting mailbox provider that sees email with your From domain.
- Daily by default, adjustable with ri= tag.
  
  Hourly: ri=3600

XML Format

- Organized by sending IP address
- Contains
  - Authentication Results (DKIM, SPF)
  - Alignment Results
  - Policy actions taken
  - Reasons for not taking policy actions

Just publish a record to see one
XML Format

The policy they found.
<policy_published>
  <domain>facebookmail.com</domain>
  <adkim>r</adkim>
  <aspf>r</aspf>
  <p>reject</p>
  <sp>none</sp>
  <pct>100</pct>
</policy_published>
DMARC Spec – Reporting

XML Format
An example record.

```
<record>
  <row>
    <source_ip>106.10.148.108</source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>facebookmail.com</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>facebookmail.com</domain>
      <result>pass</result>
    </dkim>
    <spf>
      <domain>NULL</domain>
      <result>none</result>
    </spf>
  </auth_results>
</record>
```
DMARC Spec – Reporting

Forensic Reports

• One per DMARC failure

• AFRF or IODEF formats

• Should include ‘call-to-action’ URIs

• Throttling

• Privacy issues
  • Might be redacted
  • Might not be supported
DMARC Spec – Reporting

DMARC URLs

Advertise the maximum report size a destination URI will accept

mailto:aggregate@example.com!25M

Works for both report types.
Verifying 3rd party report destinations

If the record for example.com contains reporting URIs at other domains:

```
mailto:aggregate@foo.com
```

Report generators should verify that foo.com expects the reports by looking for:

```
example.com._report._dmarc.foo.com
```

The 3rd party can change the URI to a different address in their domain:

```
v=DMARC1; rua=mailto:reports@foo.com
```
This has been the fourth of six DMARC video segments

View the entire

M³AAWG DMARC Training Series

from the public training video pages on the M³AAWG website at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Our thanks to Michael Adkins, Paul Midgen and DMARC.org
for developing the material in this series
and allowing M³AAWG to videotape it for professionals worldwide.

This video is presented by the
Messaging, Malware and Mobile Anti-Abuse Working Group

© slide PDF files and video copyrighted by the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)
For information about M³AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

Contact us at:
https://www.m3aawg.org/contact_form