Designing an open source DMARC aggregation tool.

Yadvir Singh

University of Amsterdam

June 30, 2016

Supervised by
Michiel Leenaars
Introduction

- Domain owner receives daily DMARC reports
- Difficult to process by hand
- Organize reports into a clear overview

Research question
How can aggregated DMARC reports provide domain administrators insight into their email domain?
DMARC record

v=DMARC1 p=none sp=none rua@mailto:rua@dmarc-research.nl ruf@mailto:ruf@dmarc-research.nl rf=afrf pct=100 ri=86400
DMARC Report

<report_metadata>
  <org_name>acme.com</org_name>
  <email>noreply-dmarc-support@acme.com</email>
  <extra_contact_info>http://acme.com/dmarc/support</extra_contact_info>
  <report_id>9391651994964116463</report_id>
  <date_range>
    <begin>1335571200</begin>
    <end>1335657599</end>
  </date_range>
</report_metadata>
<table>
<thead>
<tr>
<th>source_ip</th>
<th>192.0.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>2</td>
</tr>
<tr>
<td>policy_evaluated</td>
<td></td>
</tr>
<tr>
<td>disposition</td>
<td>none</td>
</tr>
<tr>
<td>dkim</td>
<td>fail</td>
</tr>
<tr>
<td>spf</td>
<td>pass</td>
</tr>
</tbody>
</table>
Tools

Commercial parties

- Several commercial parties
  - Dmarcian
  - Dmarcanalyzer
  - Agari
  - ...

- Security concerns

- No Open source alternative
Tools

Setup

- Back end: 100 % Python
- Front end: Bootstrap + Javascript
- MySQL database

- Test domain: dmarc-research.nl
- SMTP server: Postfix
- OpenDMARC, OpenDKIM, pypolicyd-spf
## Tools

### Implementation 1

### DMARC deployer

**Phase 1**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Email Volume</th>
<th>DMARC record</th>
</tr>
</thead>
<tbody>
<tr>
<td>msn.com</td>
<td>3</td>
<td>&quot;v=DMARC1; p=none; pct=100; rua=<a href="mailto:d@rua.agari.com">mailto:d@rua.agari.com</a>; fo=1&quot;</td>
</tr>
<tr>
<td>google.com</td>
<td>1</td>
<td>&quot;v=DMARC1; p=reject; rua=<a href="mailto:mailauth-reports@google.com">mailto:mailauth-reports@google.com</a>&quot;</td>
</tr>
<tr>
<td>microsoft.com</td>
<td>1</td>
<td>&quot;v=DMARC1; p=quarantine; pct=1; rua=<a href="mailto:d@rua.agari.com">mailto:d@rua.agari.com</a>,<a href="mailto:dmarc_agg@auth.returnpath.net">mailto:dmarc_agg@auth.returnpath.net</a>; ruf=<a href="mailto:d@ruf.agari.com">mailto:d@ruf.agari.com</a>; fo=1&quot;</td>
</tr>
<tr>
<td>gmail.com</td>
<td>3</td>
<td>&quot;v=DMARC1; p=none; rua=<a href="mailto:mailauth-reports@google.com">mailto:mailauth-reports@google.com</a>&quot;</td>
</tr>
<tr>
<td>os3.nl</td>
<td>7</td>
<td>None</td>
</tr>
<tr>
<td>posteo.net</td>
<td>1</td>
<td>None</td>
</tr>
</tbody>
</table>
Tools
Implementation 2

DMARC deployer
Phase 2

Trusted hosts

Foreign hosts

Yadvir Singh (University of Amsterdam)  Designing an open source DMARC aggregation tool.  June 30, 2016 9 / 17
Tools

Implementation 2

Status

**DMARC status**

- Policy configured
- Sub-policy configured
- RUA configured
- RUF configured
- PCT configured

**DMARC record**

```
v=DMARC1; p=none; sp=none; rua=mailto:r
```

DMARC test

**Result**

- Subject: The contents of
- DKIM check passed
- SPF check passed
- 4-sender SPF authorized
- DMARC check passed
Tools
Implementation 2

**Trusted hosts**

<table>
<thead>
<tr>
<th>IP address: 145.100.104.165</th>
<th>10</th>
</tr>
</thead>
</table>

- **12** DKIM pass (86.0%)
- **14** SPF pass (100.0%)
- **14** Total count

- **2** DKIM fail (14.0%)
- **0** SPF fail (0.0%)
- **14** DMARC compliant (100.0%)

Graph showing DMARC compliance trends over time.
Visualization

- Visualize incoming & outgoing DMARC reports
- Insight into domain abuse
  - by Domain
  - by IP address
Visualization

Heatmap

Yadvir Singh (University of Amsterdam)  Designing an open source DMARC aggregation tool.  June 30, 2016  14 / 17
Visualization

Bubblechart
Conclusion

- DMARC reports can give domain owners insight into their security configuration
- Can provide insights into domain abusage
- Track domain health over longer timespans.
Questions

1. https://dmarc.org/
2. https://dmarc.org/overview/