Designing an open source DMARC aggregation tool.

Yadvir Singh

University of Amsterdam

June 30, 2016

Supervised by
Michiel Leenaars

Introduction

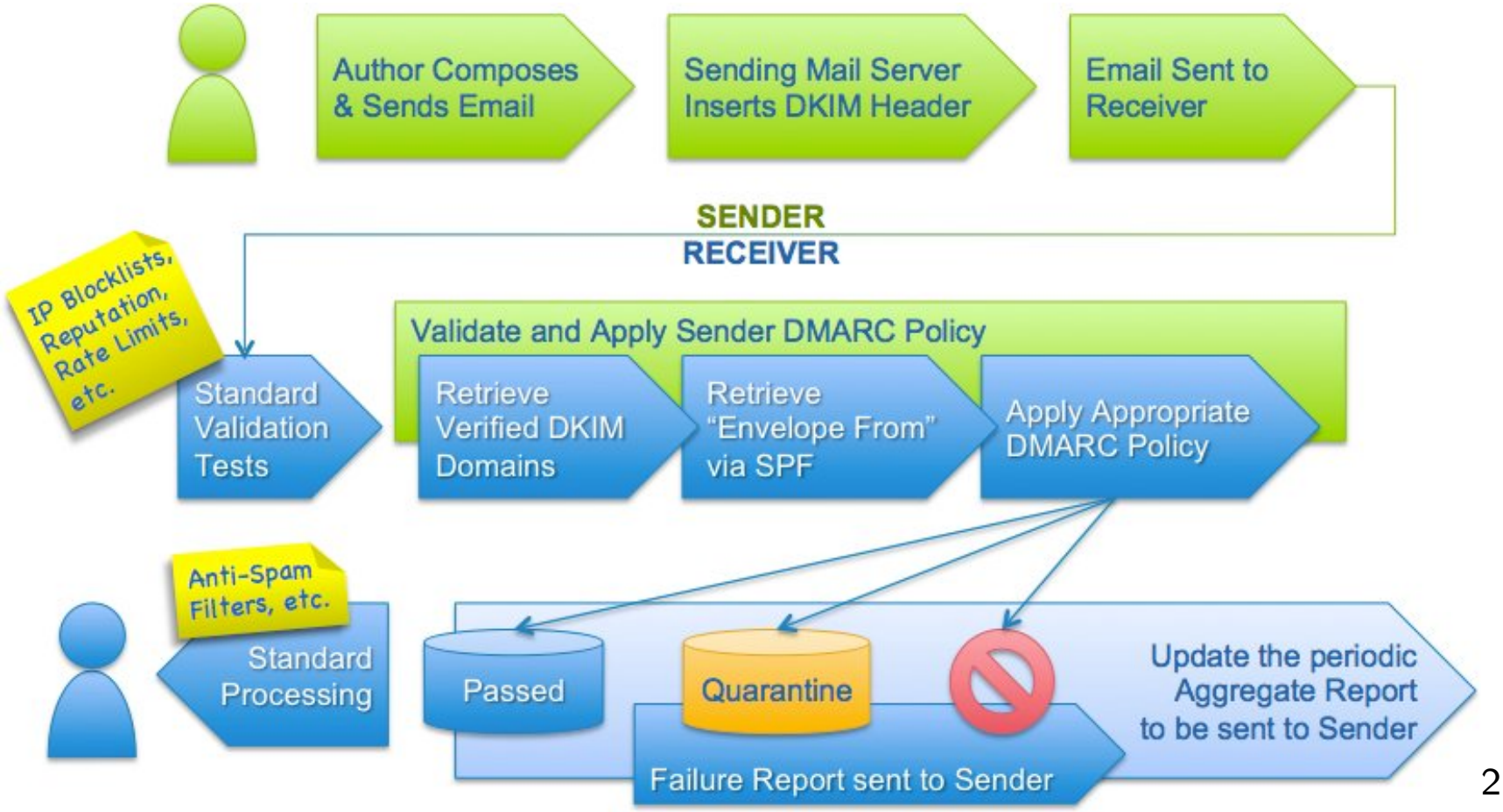
- Domain owner receives daily DMARC reports
- Difficult to process by hand
- Organize reports into a clear overview

[1]

Research question

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

DMARC



2

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>
```

DMARC

Report

```
<row>
      <source_ip>192.0.0.1</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
```

Tools

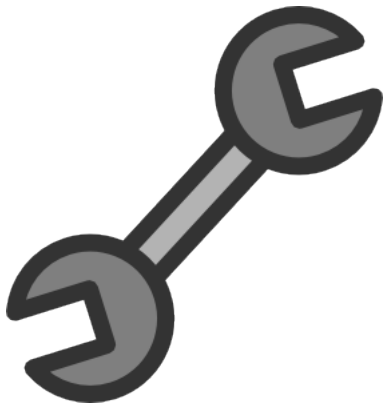
Commercial parties

- 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

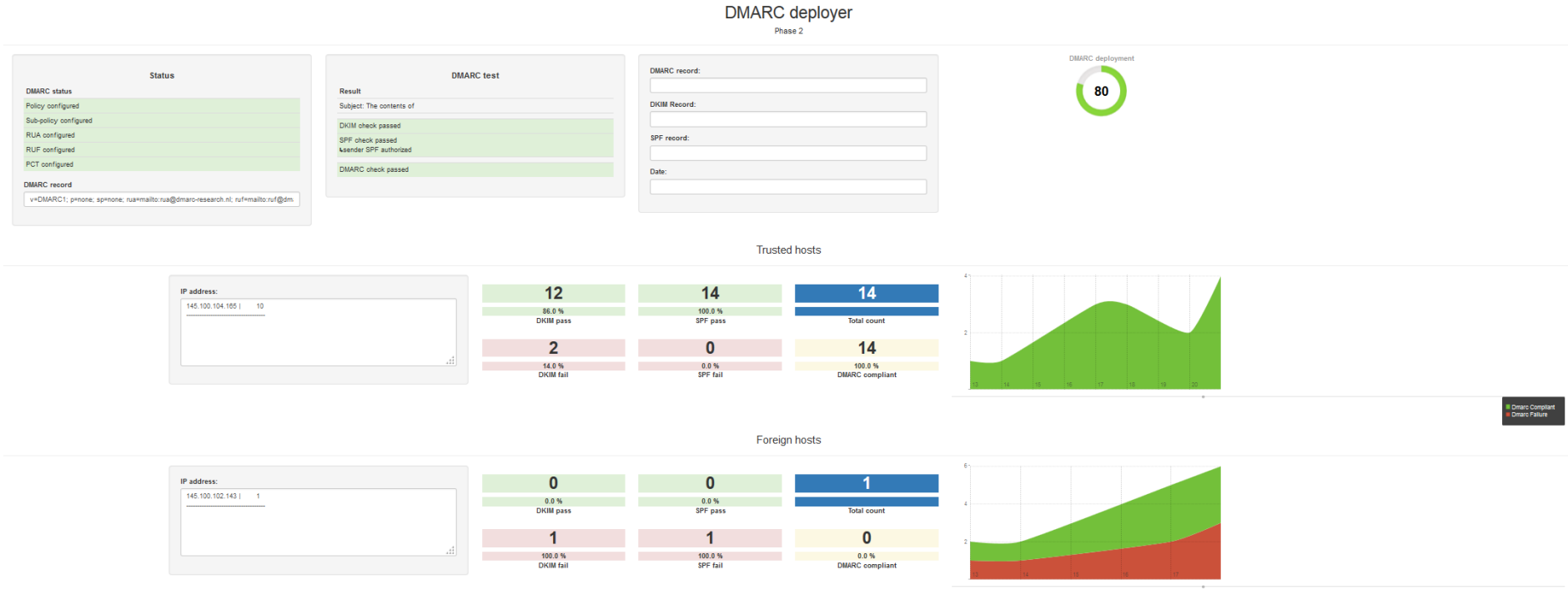
Phase 1

16	6	4	2
Emails	Domains	DMARC record published	No DMARC record published

Domain	Email Volume	DMARC record
msn.com	3	"v=DMARC1; p=none; pct=100; rua=mailto:d@rua.agari.com; fo=1"
google.com	1	"v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com"
microsoft.com	1	"v=DMARC1; p=quarantine; pct=1; rua=mailto:d@rua.agari.com,mailto:dmarc_agg@auth.returnpath.net; ruf=mailto:d@ruf.agari.com; fo=1"
gmail.com	3	"v=DMARC1; p=none; rua=mailto:mailauth-reports@google.com"
os3.nl	7	None
posteo.net	1	None

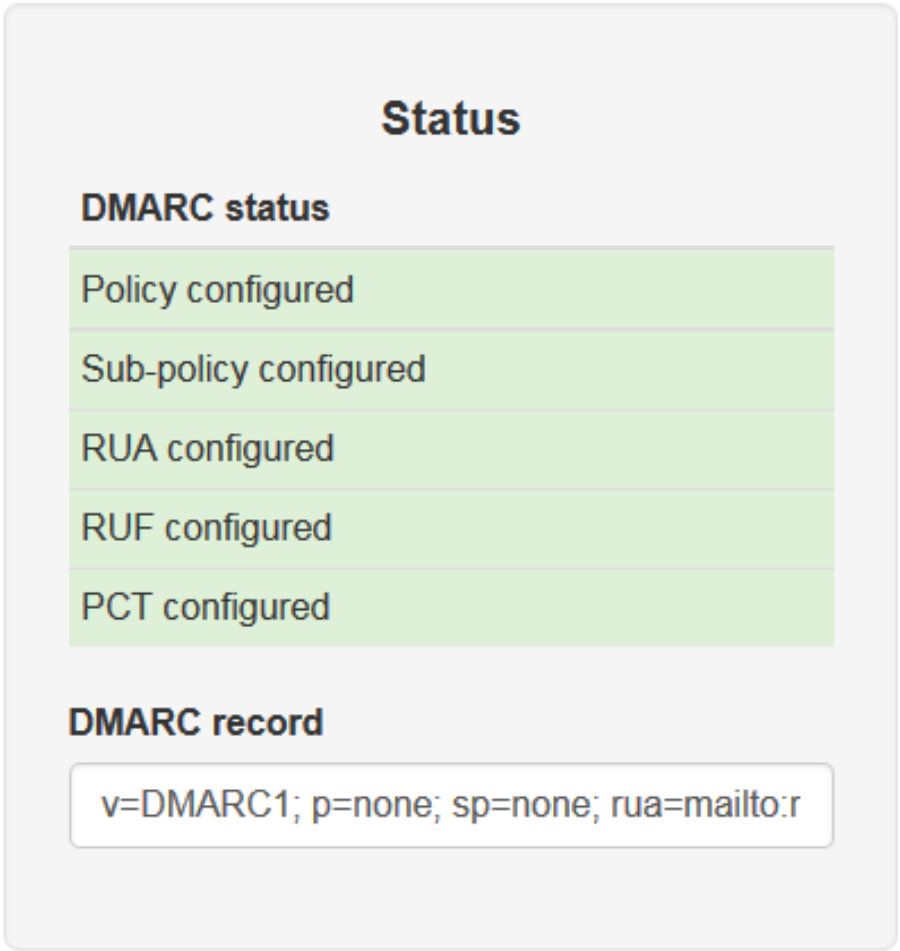
Tools

Implementation 2



Tools

Implementation 2

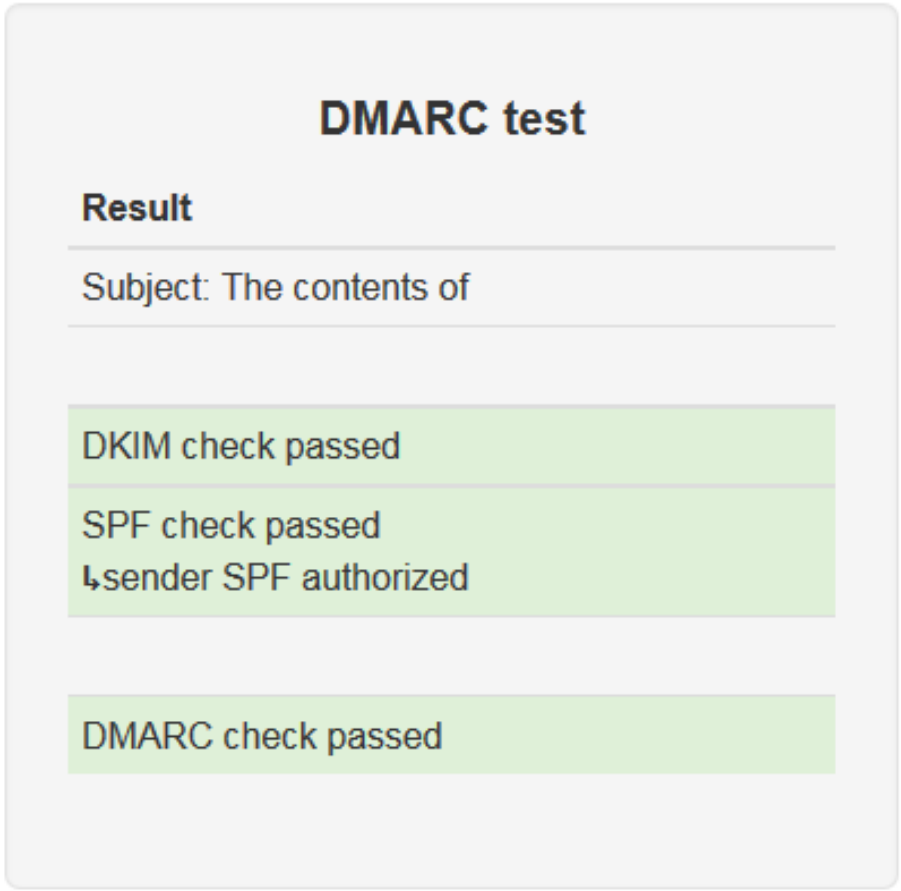


Status

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 ↳sender SPF authorized
DMARC check passed

Tools

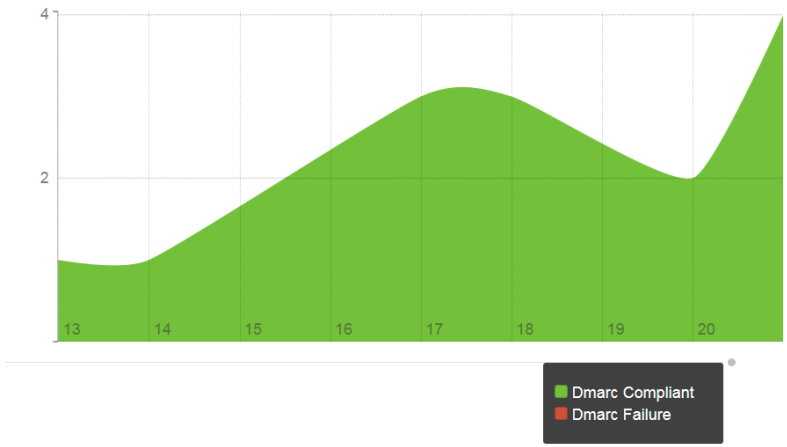
Implementation 2

Trusted hosts

IP address:

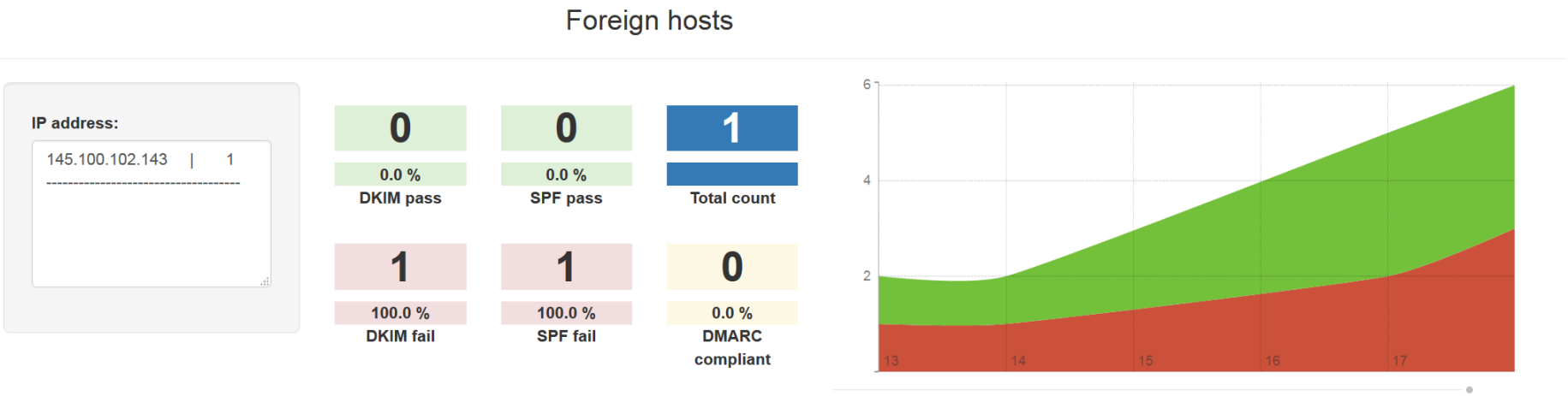
145.100.104.165 | 10

12	14	14
86.0 %	100.0 %	
DKIM pass	SPF pass	Total count
2	0	14
14.0 %	0.0 %	100.0 %
DKIM fail	SPF fail	DMARC compliant



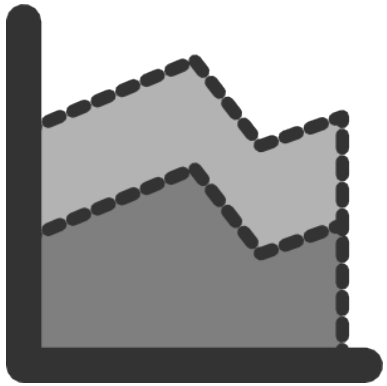
Tools

Implementation 2



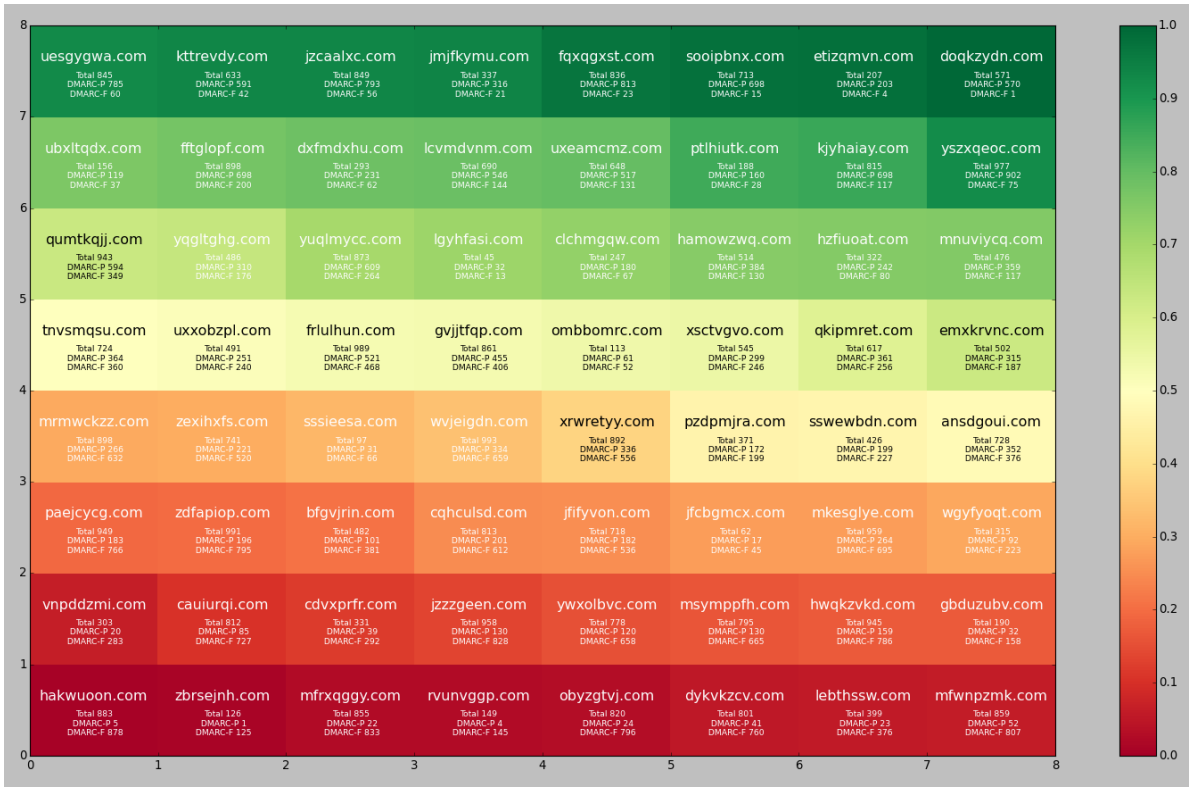
Visualization

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



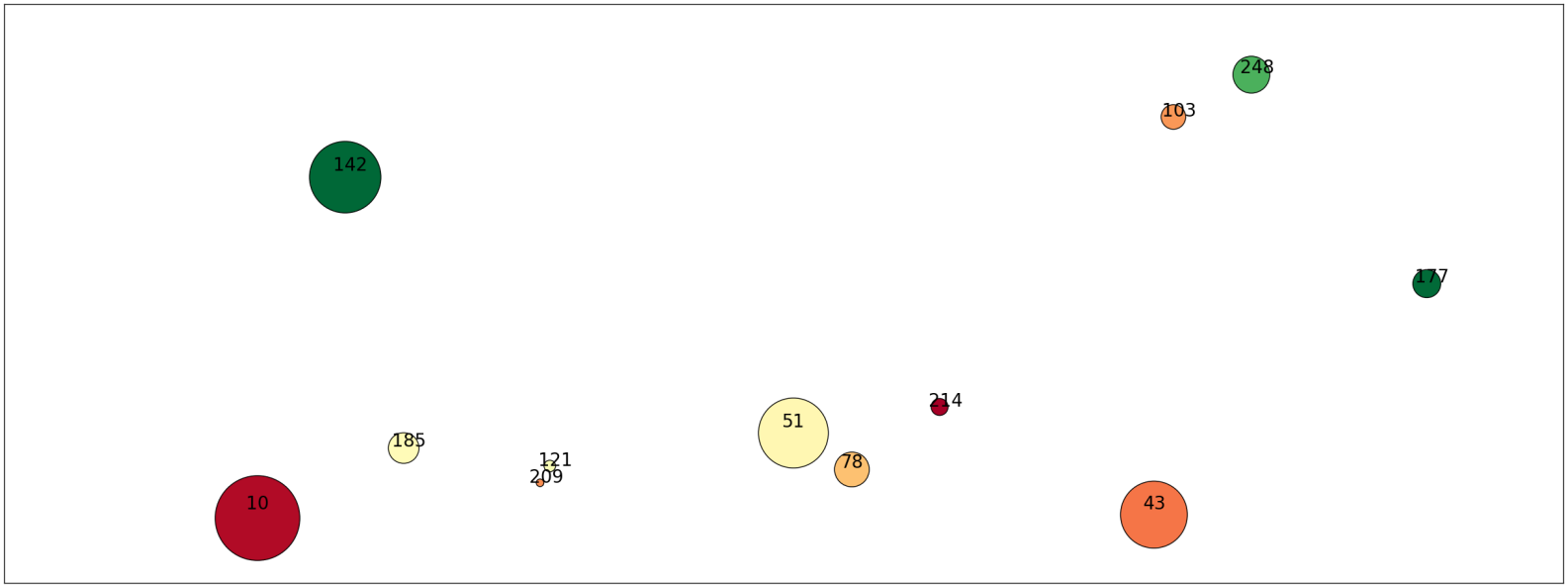
Visualization

Heatmap



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/