You’ve Got Report: Measurement and Security Implications of DMARC Reporting

Md. Ishtiaq Ashiq§, Weitong Li§, Tobias Fiebig†, and Tijay Chung§

§Virginia Tech, †Max Planck Institute for Informatics
How Email Works

MUA_s → SMTP/HTTP → MTA_s → SMTP → MTA_R → LMTP → MDA → Mailbox

DNS

Who is the recipient MTA?
How SMTP Works

MUA ➔ SMTP/HTTP ➔ Sending MTA ➔ SMTP ➔ Recipient MTA ➔ LMTP/SMTP ➔ MDA

- How can recipient authenticate the sending domain?
  - HELO example.com
  - MAIL FROM: <foo@example.com>
  - RCPT TO: <bar@example.net>
  - DATA ...

Sender Authentication

SPF
DKIM
DMARC
SPF (Sender Policy Framework)

192.0.2.3

example.com

1

example.net

Is 192.0.2.3 authorized to use “example.com” as its MAIL FROM domain?
SPF (Sender Policy Framework)

example.com

192.0.2.3

v=spf1 ip4:192.0.2.0/24 -all

example.com

MAIL FROM

example.com

DNS Resolver

example.net
DKIM (DomainKeys Identified Mail)

default._domainkey.example.com TXT
k=rsa; p=MIGfMAMIGfMA0MIGfMIGfMIGfMIGfMAGCd...

example.com

example.net

SMTP

DNS Auth.

DNS Resolver
What happens if SPF/DKIM validation fails?

• SPF/DKIM do not tell what actions the receiver has to take when validation fails.
DMARC
(Domain-based Message Authentication, Reporting & Conformance)

SMTP

DNS Auth.

example.com

example.net

_v=dmarc.example.com TXT v=DMARC1; p=reject;
DMARC
(Domain-based Message Authentication, Reporting & Conformance)

Contains lots of meta information like source IP, evaluated policy, results, the number of emails, and so on.
DMARC
(Domain-based Message Authentication, Reporting & Conformance)

- Helps sender identify and address threats promptly
DMARC
(Domain-based Message Authentication, Reporting & Conformance)

- XML formatted, thus not user-friendly – thus 80% of the report recipient address is an external domain.
DMARC report w/ external domains

SMTP  
DNS

_dmarc.example.com
TXT  v=DMARC1; p=reject; rua=mailto:report@example.org

example.com
SMTP
DNS Auth.

example.net
SMTP
DNS Resolver

example.org
SMTP
DNS Auth.

How does example.net know that example.org has agreed to receive the report?
DMARC report w/ External Destination Verification (EDV)

 SMTP  DNS  example.com
   |     | SMTP
   |     | DNS Auth.
   | 1   | DMARC
   |     | DNS Resolver
   | 2   | EDV
   |     | example.net
   | SMTP| 4
   | DNS Auth.|
   | example.org

_dmarc.example.com  TXT  v=DMARC1; p=reject; rua=mailto:report@example.org

example.com._report._dmarc.example.org  TXT  v=DMARC1
SMTP TLS Reporting

- Senders compatible with MTA-STS or DANE can share success and failure statistics with the receivers

- Helps receivers fix their TLS configuration, MTA-STS or DANE policy, etc.

_TLSMTP_tls.example.net TXT v=TLSRPTv1; rua=mailto:report@example.org

TLS miscon��uration, policy errors, etc.
Research Questions

Measurement

- How many domains use DMARC?
- How many of them use DMARC Reporting?
- How many receivers send DMARC reports?
Status Quo (all domains)

More than 50% of them uses DMARC reporting

The majority specify external domains to receive and process the report
Nearly 20% of domains that use external domains, do not have EDV authorization record. Again, more than 50% of them uses DMARC reporting.
Research Questions
Attacker’s Perspective
Misconfigurations?

• Do SMTP servers in the wild have EDV check?

• How about popular email hosting providers?
Ambiguities?

• Do SMTP servers in the wild have EDV check?
  • How about popular email hosting providers?

• Is RFC 7489 unambiguous for reporting?
  • What happens when there are duplicate addresses in rua tag?
  • Is there a limit to the number of addresses in rua tag?
# Experiments

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Type</th>
<th>RData</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exp. 1</td>
<td>_dmarc.a.com</td>
<td>TXT</td>
<td>v=DMARC1; p=none; rua=<a href="mailto:admin1@a.com">mailto:admin1@a.com</a>, ... , <a href="mailto:admin50@a.com">mailto:admin50@a.com</a></td>
</tr>
<tr>
<td>Exp. 2</td>
<td>_dmarc.a.com</td>
<td>TXT</td>
<td>v=DMARC1; p=none; rua=<a href="mailto:admin@a.com">mailto:admin@a.com</a>, ... , <a href="mailto:admin@a.com">mailto:admin@a.com</a></td>
</tr>
<tr>
<td>Exp. 4</td>
<td>_dmarc.a.com</td>
<td>TXT</td>
<td>v=DMARC1; p=none; rua=<a href="mailto:admin@a.com">mailto:admin@a.com</a>, <a href="mailto:admin@b.com">mailto:admin@b.com</a></td>
</tr>
<tr>
<td>Exp. 6</td>
<td>_dmarc.a.com</td>
<td>TXT</td>
<td>v=DMARC1; p=none; rua=<a href="mailto:admin@a.com">mailto:admin@a.com</a></td>
</tr>
<tr>
<td></td>
<td>_smtp._tls.a.com</td>
<td>TXT</td>
<td>v=TLSRPTv1; rua=<a href="mailto:admin@b.com">mailto:admin@b.com</a></td>
</tr>
</tbody>
</table>
## Result

<table>
<thead>
<tr>
<th>EHP</th>
<th>Report Size (B)</th>
<th># of addr.</th>
<th>EDV</th>
<th>Duplication Check</th>
<th>SMTP TLS Reporting (Exp. 6)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Check (Exp. 4)</td>
<td>Addr. (Exp. 2)</td>
</tr>
<tr>
<td>Google</td>
<td>3,962</td>
<td>50</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Yahoo</td>
<td>4,626</td>
<td>50</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>QQ</td>
<td>3,628</td>
<td>50</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>FastMail</td>
<td>4,839</td>
<td>10</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>OpenDMARC</td>
<td>2,238</td>
<td>8-12*</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Rspamd</td>
<td>2,320</td>
<td>50</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

* OpenDMARC restricts DNS records to a maximum of 255 characters.
Google Workspace, Yahoo, and QQ do not check EDV and do not have duplication check; So, amplification factor achievable by using them as reflector is 950x, 1150x, and 900x
Google workspace can be used as a reflector and achievable amplification factor is 1,460x
Conclusion

• First comprehensive study of the DMARC reporting ecosystem
  
  • DMARC reporting and the lived practice of how it is implemented—holds the potential for annoying Denial-of-Service attacks
  
  • SMTP TLS reporting can also be combined to raise the attack factor
  
  • Qualitative study
  
  • Recommendations for future iterations on RFC7489