Email Authentication and Related Standards

DMARC.org and LinkedIn

Steven M Jones
BIMI Background
What Is BIMI?

Senders may have logos they control displayed with their messages.
Origins of BIMI

• 2015: Microsoft and GMail both start to display logos in (mobile) mail programs
• Logos taken from various internal sources
• Neither company wants to manage other people’s logos

• Working group proposed under DMARC.org
• Just like a FAVICON.ICO for email (at first)
• First meeting held at the M3AAWG 34 in Dublin on June 11\textsuperscript{th}
• Standalone group created at the end of 2016
Requirements To Use BIMI

• Deploy DMARC with “quarantine” or “reject” policy
• Publish an additional BIMI record in DNS
• Publish SVG logo image on a web server

• For Google you must obtain a special X.509 certificate
  • Verified Mark Certificate (VMC)
  • Two vendors, DigiCert and Entrust Datacard (MVA)
  • Must submit proof of trademark ownership
  • Include link to VMC in BIMI DNS record
## Where Is BIMI Today?

<table>
<thead>
<tr>
<th>Supports BIMI</th>
<th>Considering BIMI</th>
<th>Does not support BIMI</th>
</tr>
</thead>
<tbody>
<tr>
<td>yahoo! - AOL</td>
<td>1&amp;1 mail.com GMX</td>
<td>Apple</td>
</tr>
<tr>
<td>Google Gmail</td>
<td>BT Outlook Office365</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Fastmail Pobox</td>
<td>COMCAST</td>
<td>Yahoo</td>
</tr>
</tbody>
</table>

Source: bimigroup.org
More Information About BIMI

• JPAAWG 4 Sessions:
  • A1-4 これから始めるBIMI
  • A2-4 電子メール認証技術最先端領域
  • B2-5 あなたの組織をなりすましから保護するための技術を紹介

• Other Resources:
  • BIMI Group – www.bimigroup.org
  • Wikipedia - en.wikipedia.org/wiki/Brand_Indicators_for_Message_Identification
  • Many helpful pages and videos from vendors, check YouTube and bimigroup.org/videos/
Other Developments
DMARC Reporting

- Microsoft stopped sending aggregate reports in 2017
- Microsoft **resumed** sending aggregate reports mid-2021
  - Limited to Hotmail, Live.com, MSN.com, Outlook.com
- Some formatting issues (main body encoding, too-long lines)

- No timeline for reporting from Office 365
What Is ARC?

Authenticated Received Chain (ARC)

• When a message is forwarded, email authentication is frequently broken

• ARC allows the forwarder to convey the authentication results as they received the message

• Recipients of forwarded messages with ARC headers can see if the message passed authentication when the forwarder received it

• If forwarder has good reputation, receiver may choose to accept their authentication results
Who Is Using ARC?

• ARC sealing messages
  • Google Groups
  • Outlook.com
  • Office 365
  • Fastmail
  • Strato.com (European hosting company)

• Two companies validating ARC on incoming messages
  • Large customer management (CRM) company
  • German company: About 10% of messages that failed normal authentication checks are “recovered” by validating ARC
What Happened To TLS 1.3?

• TLS 1.2 and earlier are vulnerable

• What are the advantages of TLS 1.3?
  • Much faster initial handshakes – half the time, milliseconds/connection
  • More secure encryption algorithms
  • More resistant to Man-In-The-Middle attacks

• Fairly good adoption due to CDNs, service providers
• Still need to fallback for consumers, small organizations

• Need to encourage adoption – see Open Round Table #1
IETF Activity
DMARC Working Group News

• DMARC policies for Public Suffix Domains (PSD) published as RFC9091 in July 2021
  • United States published policy for .gov TLD in October
  • United Kingdom published policy for gov.uk
  • No data shared yet, maybe at M3AAWG 54 (February)

• No traction for Author: and Sender: drafts from 2020
  • Both addressed From: rewriting by mailing lists
Agenda for DMARC at IETF 112

- Methods to locate a domain’s DMARC policy
  - How to find the Organizational Domain (OD)
  - RFC7489 references the Public Suffix List (PSL) from Mozilla
- Proposal to move OD discovery to a separate document
- Proposal to simplify OD discovery by doing more DNS lookups (“walk the tree”)
- Some proposals related to indirect mail flows (mailing lists) and ARC may be discussed
EmailCore Working Group

• Developing updates to RFC5321 and RFC5322

• Proposal to make these features mandatory:
  • 8BITMIME [RFC 6152]
  • Enhanced Reply Codes [RFC 5248]
  • Delivery Status Notification (DSN) [RFC 3461]

• Proposal to make these features strongly recommended:
  • PIPELINING [RFC 2920]
  • SMTPUTF8 [RFC 6531]
JMAP Working Group

- JSON Meta Application Protocol (JMAP)
- Access and synchronize email, calendar, contacts

- A number of RFCs published since 2019
  - RFC 8620 JMAP core
  - RFC 8621 JMAP for mail
  - RFC 8887 and RFC 9007

- Working on multiple documents at IETF 112
  - S/MIME (encrypted/signed message) support
  - Calendar, Task, and Contact objects
About This Data

- Raw data supplied by Farsight Security
- DNS request/response data captured from sensors widely deployed across the Internet
- Not 100% coverage of Internet, but a stable sensor network useful for comparisons over time
- DMARC.org thanks Farsight for their continuing support
Active DMARC Records and % Growth By Month

Total Records: 4,443,457
Total Active DMARC Records By Period

- 2016-12: 80,275
- 2017-06: 134,280
- 2017-12: 240,151
- 2018-06: 342,367
- 2018-12: 630,000
- 2019-06: 1,084,767
- 2019-12: 1,892,227
- 2020-06: 2,221,962
- 2020-12: 2,704,575
- 2021-06: 3,461,520
- 2021-09: 4,443,457
DMARC Policies

<table>
<thead>
<tr>
<th>Date</th>
<th>p=reject, 23.5%</th>
<th>p=quarantine, 10.9%</th>
<th>p=none, 65.6%</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021-09</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DMARC Policies By Year
Active BIMI Records

- Total BIMI records observed: 9,860
- Including link to a VMC: 179
- Many large brands with a VMC:

  - Pinterest
  - UPS
  - Ericsson
  - CNN

  - JPMorgan Chase & Co.
    - 18 records

  - eBay
  - Disney+
  - Bank of America
Monthly New BIMI Records

- 2021-03: 672
- 2021-04: 383
- 2021-05: 672
- 2021-06: 500
- 2021-07: 922
- 2021-08: 762
- 2021-09: 533
DKIM Signing Algorithms

• DKIM specified with RSA signature algorithm (2007)

• RFC 8463 (2018) describes Elliptic Curve algorithm for DKIM signatures (Ed25519-SHA256)

• Common problem with DKIM deployment: DNS TXT record too long for vendor’s GUI

• Smaller keys provide equivalent strength against brute force attack

• Room to scale keys against quantum computing attacks
RSA Key vs. Ed25519 Key

• DKIM key record for 2,048 bit RSA key

test._domainkey.football.example.com. IN TXT ( "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDkH1OQoBTzWR" "iGs5V6Np3idY6Wk08a5qhdR6wy5bdOKb2jLQiY/J16JYi0Qvx/byYzCNb3W91y3FutAC" "DfzwQ/BC/e/8uBsCR+yz1Lxj+PL6lHvqMKrM3rG4hstT5QjvHO9PzoxZyVYLzBfO2EeC3" "Ip3G+2kryOTIKT+1/K4w3QIDAQAB" )

• DKIM key record for 256 bit Ed25519 key

brisbane._domainkey.football.example.com. IN TXT ( "v=DKIM1; k=ed25519; p=11qYAYKxCrfVS/7TyWQHOg7hcVPapiMlrwIaaPcHURo=" )
How Common Is Ed25519?

• Ed25519 keys: 1,775 (2,019 since 2018)
• RSA keys: 7,699,768 (38+MM since 2010)

• Answer: Not very common (yet)

• Why so few Ed25519 keys after three years?
  • Missing software support? Upgrades needed?
  • How many domains use an ESP’s keys and software?
  • Perhaps promote Ed25519 with TLS 1.3 upgrade?
DKIM RSA Key Lengths (2021)

Keys

<table>
<thead>
<tr>
<th>Key Length (bits)</th>
<th>Number of Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>384</td>
<td>163</td>
</tr>
<tr>
<td>512</td>
<td>357</td>
</tr>
<tr>
<td>768</td>
<td>7,361</td>
</tr>
<tr>
<td>1,024</td>
<td>2,602,612</td>
</tr>
<tr>
<td>1,536</td>
<td>108</td>
</tr>
<tr>
<td>1,792</td>
<td>82</td>
</tr>
<tr>
<td>2,048</td>
<td>4,977,039</td>
</tr>
<tr>
<td>3,072</td>
<td>42</td>
</tr>
<tr>
<td>4,096</td>
<td>3,563</td>
</tr>
<tr>
<td>8,192</td>
<td>3</td>
</tr>
<tr>
<td>20,048</td>
<td>1</td>
</tr>
</tbody>
</table>
Thank you