Extended Hell(o):
A Comprehensive Large-Scale Study on Email Confidentiality and Integrity Mechanisms in the Wild

Birk Blechschmidt* and Ben Stock*

*Saarland University  *CISPA Helmholtz Center for Information Security

32nd USENIX Security Symposium
Background: Email Security Mechanism Evolution

- STARTTLS
- SPF
- DKIM
- DANE
- DANE-TLSA
- DANE OpenPGP
- DMARC
- MTA-STS

Sender-domain auth.  MTA to MTA encr. and auth.  E2E encr. and auth.
Measurement Methodology

Domain-scoped tests (10M)
- SPF and DMARC
- MTA-STS
- OPENPGPKEY and SMIMEA

MX-scoped tests (2.5M)

Inbound scenarios
- SPF, DKIM and DMARC misconfigurations

Provider-scoped tests (47)

STARTTLS and DANE-TLSA measurement

Outbound scenarios
- DANE-TLSA and MTA-STS misconfigurations
### Provider Scoped Results: SPF, DKIM and DMARC

<table>
<thead>
<tr>
<th>Scenario</th>
<th>gmail.com</th>
<th>sapo.pt</th>
<th>zoho.com</th>
<th>tutanota.com</th>
<th>vodafone.de</th>
</tr>
</thead>
<tbody>
<tr>
<td>No SPF, DMARC Reject, no DKIM</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>SPF fail, DMARC Reject, DKIM key unpublished</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>SPF fail, DMARC Quarantine, DKIM key unpublished</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>DMARC Parent Reject</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Double From 1</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Double From 2</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

- Few providers provide satisfying security
- As a sender, implementing a single mechanism is not sufficient
- We can produce UI mismatches through double From headers in three providers supporting DMARC
- DMARC’s parent reject policy is sometimes not implemented correctly
- Some providers with no filtering or proprietary mechanisms (e.g. IP address reputation)
**Provider-Scoped Results: TLS & DANE-TLSA**

<table>
<thead>
<tr>
<th>Providers</th>
<th>STARTTLS</th>
<th>TLSA requested</th>
<th>TLSA implies STARTTLS</th>
<th>Allowing for unencrypted outbound mail</th>
<th>Accepting invalid certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>42</td>
<td>10</td>
<td>8</td>
<td>45</td>
<td>40</td>
</tr>
</tbody>
</table>

Birk Blechschmidt – Extended Hell(o) – USENIX Security ’23
MX-Scoped Results: TLS certificates

- 30% of certificates fail validation

STARTTLS Measurement

- Self-signed certificate
- Expired certificate
- Missing certificate in the chain
- Only hostname mismatch
- Hostname mismatch
- Total failed validations
How to transmit emails securely between MTAs

- Each MX should have a TLSA record (9,480 records of 2.5M MX records)

- TLSA must be DNSSEC-signed (8,398 servers remaining)
  - 8,176 servers responsible for 117,126 domains have a matching TLSA record

- But: domains’ MX records must also be protected by DNSSEC
  - only 71,176 domains which really benefit
Domain-Scoped Results: OPENPGPKEY and SMIMEA

- DNS Empty Non-Terminals allow us to find potentially supporting domains
  - If anything._openpgpkey.example.org exists, _openpgpkey.example.org does not return NXDOMAIN
- NSEC zones allow for trivial key strength measurement
  - We use a custom hashcat module for cracking zones with NSEC3
- Mostly used by specialized entities well-known in the tech community
  - 100 OPENPGPKEY and 26 SMIMEA supporting zones

![OpenPGP keys chart](chart.png)

- OpenPGP keys
- RSA 4096
- DSA 1024
- RSA 2048
- Elgamal 2048
- RSA 1024
- Elgamal 1024
- RSA 3072
- Elgamal 4096
- Ed25519
- Curve25519
- RSA 1024
Conclusion

• We all use email every day, yet it suffers from severe deficiencies

• Providers lack behind in implementation of security checks (e.g., only 7/46 support TLSA, all allow unencrypted outgoing connections)

• Ecosystem shows TLS certificates are not well-managed

• Complexity of DNSSEC and plethora of protocols as major hindrances to security

• Automated end-to-end encryption is futile and badly implemented