Neither Snow Nor Rain Nor MITM...
An Empirical Analysis of Email Delivery Security

Nicolas Lidzborski, Elie Bursztein, Kurt Thomas, Vijay Eranti (Google)
Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, J. Alex Halderman (University of Michigan) Michael Bailey (University of Illinois)
Study's goal: measuring the state of email delivery security
Agenda

Email encryption while in transit
Current deployment of SMTP TLS and attacks observed in the wild

Email authentication
How prevalent authentication technologies are

The future of email security
Overview of on-going efforts dedicated to improve email security
Datasets used in the study

Gmail longitudinal data
Longitudinal statistics based on what Gmail sees

Alexa top 1M sites
Zmap scanning of Alexa Top 1M sites SMTP servers

IPv4 public SMTP and DNS servers
Zmap scanning for publicly reachable SMTP & DNS servers
SMTP encryption
SMTP encryption

Sender (Alice) → Mail server (smtp.source.com) → Mail server (smtp.destination.com) → Recipient (Bob)

MX: IP:1.2.3.4

Eavesdropper (Eve)

DNS server

Recipient

Mail server

Mail server

IP:1.2.3.4

MX

DNS server

Sender

Eavesdropper

Recipient

Mail server
Fraction of email encrypted as seen by Gmail
## Encryption quality

<table>
<thead>
<tr>
<th>Provider</th>
<th>Incoming Key Exchange</th>
<th>Certificate name</th>
<th>Incoming ciphersuite</th>
<th>Outgoing key exchange</th>
<th>Outgoing ciphersuite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail</td>
<td>ECDHE</td>
<td>match</td>
<td>AES128-GCM</td>
<td>ECDHE</td>
<td>AES128-GCM</td>
</tr>
<tr>
<td>Yahoo</td>
<td>ECDHE</td>
<td>match</td>
<td>AES128-GCM</td>
<td>ECDHE</td>
<td>RC4-128</td>
</tr>
<tr>
<td>Microsoft</td>
<td>ECDHE</td>
<td>match</td>
<td>AES256-CBC</td>
<td>ECDHE</td>
<td>AES256</td>
</tr>
<tr>
<td>Apple iCloud</td>
<td>ECDHE</td>
<td>match</td>
<td>AES128-GCM</td>
<td>DHE</td>
<td>AES128-GCM</td>
</tr>
<tr>
<td>Facebook mail</td>
<td>RSA</td>
<td>mismatch</td>
<td>AES128-CBC</td>
<td>ECDHE</td>
<td>AES128-CBC</td>
</tr>
<tr>
<td>Comcast</td>
<td>RSA</td>
<td>match</td>
<td>RC4-128</td>
<td>DHE</td>
<td>AES128-CBC</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>ECDHE</td>
<td>match</td>
<td>AES128-GCM</td>
<td>ECDHE</td>
<td>RC4-128</td>
</tr>
</tbody>
</table>
STARTTLS

TCP handshake

220 Ready

EHLO

250 STARTTLS

Source mail server
(smtp.source.com)

Destination mail server
(smtp.destination.com)

220 GO HEAD

TLS negotiation

Encrypted email

Cleartext

Encrypted
STARTTLS downgrade attack

TCP handshake

220 Ready

EHLO

250 250 STARTTLS

Email in clear

Source mail server
(smtp.source.com)

Destination mail server
(smtp.destination.com)
## STARTTLS downgrade by AS / organization

<table>
<thead>
<tr>
<th>Organization Type</th>
<th>ASes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporation</td>
<td>43% (182)</td>
</tr>
<tr>
<td>ISP</td>
<td>17.5% (74)</td>
</tr>
<tr>
<td>Financial institutions</td>
<td>13.5% (57)</td>
</tr>
<tr>
<td>Academic institutions</td>
<td>8.3% (35)</td>
</tr>
<tr>
<td>Healthcare</td>
<td>3.3% (14)</td>
</tr>
<tr>
<td>Unknown</td>
<td>2.8% (12)</td>
</tr>
<tr>
<td>Airport</td>
<td>2.1% (9)</td>
</tr>
<tr>
<td>Hosting</td>
<td>1.7% (7)</td>
</tr>
<tr>
<td>NGO</td>
<td>0.7% (3)</td>
</tr>
</tbody>
</table>
STARTTLS downgrading as seen by Gmail

<table>
<thead>
<tr>
<th>country</th>
<th>% of inbound traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunisia</td>
<td>96.13%</td>
</tr>
<tr>
<td>Iraq</td>
<td>25.61%</td>
</tr>
<tr>
<td>Papua New Guinea</td>
<td>25.00%</td>
</tr>
<tr>
<td>Nepal</td>
<td>24.29%</td>
</tr>
<tr>
<td>Kenya</td>
<td>24.13%</td>
</tr>
<tr>
<td>Uganda</td>
<td>23.28%</td>
</tr>
<tr>
<td>Lesotho</td>
<td>20.25%</td>
</tr>
<tr>
<td>Sierra Leone</td>
<td>13.41%</td>
</tr>
<tr>
<td>New Caledonia</td>
<td>10.13%</td>
</tr>
<tr>
<td>Zambia</td>
<td>9.98%</td>
</tr>
<tr>
<td>Reunion</td>
<td>9.28%</td>
</tr>
</tbody>
</table>
MITM via DNS MX record hijacking

Sender (Alice) -> Mail server (smtp.source.com) -> DNS server

MX? IP: 6.6.6.6

Rogue Mail server (smtp.destination.com)

Real mail server (smtp.destination.com) -> Recipient (Bob)
DNS spoofing as seen by Gmail

<table>
<thead>
<tr>
<th>country</th>
<th>% of inbound traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slovakia</td>
<td>0.08%</td>
</tr>
<tr>
<td>Romania</td>
<td>0.04%</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>0.02%</td>
</tr>
<tr>
<td>India</td>
<td>0.01%</td>
</tr>
<tr>
<td>India</td>
<td>0.01%</td>
</tr>
<tr>
<td>Israel</td>
<td>0.01%</td>
</tr>
<tr>
<td>Poland</td>
<td>0.01%</td>
</tr>
<tr>
<td>Switzerland</td>
<td>0.01%</td>
</tr>
<tr>
<td>Ukraine</td>
<td>0.01%</td>
</tr>
<tr>
<td>Others</td>
<td>&gt;0.01%</td>
</tr>
</tbody>
</table>

Google
Email authentication
Email authentication?

Apple customers targeted by fake iTunes email scam

A phishing scam asking users to click refund links in a legitimate-appearing email purporting to be from Apple is doing the rounds.

Examples from October 2015

Phishing scam targets videogamers

Videogamers are being targeted in phishing scams looking to take advantage of their devotion to their games, the Federal Trade Commission is warning.

The scam tries to dupe players into believing the gaming companies are coming after them for such things as selling in-game characters or items used in the game for actual money, the FTC said. Fraudsters send emails to gamers claim the company is going to sue them for up to $2,700 for continued violations of using real money for in-game transactions, hoping to bait targets of the scam into sharing personal or financial information.
Email authentication technologies

SPF - Sender policy framework
Specify which IP addresses/prefix are allowed to send emails

DKIM - Domain Key Identified Email
Use public key cryptography to sign the content of emails

DMARC - Domain Message Authentication Reporting and Conformance
Specify what to do (reject, spam folder...) with non authenticated emails
Inbound authentication as seen by Gmail

2013

- No authentication: 8.7%
- SPF only: 14.4%
- DKIM only: 2.3%
- DKIM & SPF: 74.7%

2015

- No authentication: 5.6%
- SPF only: 11.4%
- DKIM only: 2.0%
- DKIM & SPF: 81.0%
Why DKIM fail?

- DNS.TXT not found: 41.11%
- Body hash did not verify: 18.66%
- Verified but weak crypto: 15.08%
- Verification failed: 10.75%
- Invalid subdomain: 5.38%
- Missing required parameters: 4.07%
- Version not supported: 3.32%
- Local part didn't match TXT: 0.46%
- Key type not implemented: 0.26%
- Signature expired: 0.06%
- Parse error -- duplicate tag: 0.05%
- Key revoked: 0.01%
Exposing data to Postmasters

**IP Reputation**
- **Volume of IPs in each Reputation Group**
  - 100%
  - 75%
  - 50%
  - 25%

**Authenticated Traffic**
- **Volume of Traffic passing Authentication**
  - DKIM success rate
  - SPF success rate
  - DMARC success rate
Future
Missing encryption UI
SMTP Strict Transport Security and cert pinning
DMARC strict rejection enforcement and Auth Chain
Thank you!