Expect Signed Mail

IETF 118
Prague
November 2023
Daniel Kahn Gillmor
e2e cryptographically signed e-mail

- Possible for decades
- Rarely used
- Rarely useful
Why send signed mail?

- Assure recipient mail came from you
- Help recipient avoid spearphishing
Why don’t people send signed mail?

- Extra hassle
- Ugly failure modes
- Might not actually help prevent spearphishing
UX, UX, UX

- User experience and user expectations are the core of the problem
What does signed mail look like?

Unannotated

Broken

Signed

Expect Signed Mail
Where have we seen this before?

<table>
<thead>
<tr>
<th>Treatment of HTTPS pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current (Chrome 67)</td>
</tr>
<tr>
<td>Secure example.com</td>
</tr>
<tr>
<td>Sep. 2018 (Chrome 69)</td>
</tr>
<tr>
<td>example.com</td>
</tr>
<tr>
<td>Eventually</td>
</tr>
<tr>
<td>example.com</td>
</tr>
</tbody>
</table>
Continuing the analogy to HTTPS...
One final HTTPS analogy

- RFC 6797 (Strict-Transport-Security, aka HSTS)
- Endpoint opts in to requiring cryptographic security
- Clients refuse to load weak transport
Best current practice

• Draft-ietf-lamps-e2e-mail-guidance: broken signatures are missing signatures

• Not universally implemented
draft-dkg-lamps-expect-signed-mail

- User signals that all mails from them will be signed
- Recipients use this signal to limit exposure to unsigned mail or mail with broken signatures
- draft-ietf-lamps-e2e-mail-guidance “Future Work” §A.8 “expectations of cryptographic protections”
Decisions

- Signal location \((e-mail\ header? \text{ Depends on draft-ietf-lamps-header-protection})\)
- Signal scope \((all\ messages \text{ From:}\ specific\ e-mail\ address)\)
- Intervening MUAs \((e.g.,\ mailing\ list\ munging)\)
- Deciding to signal \((what\ if\ I\ have\ multiple\ MUAs?)\)
- Consequences \((unsigned\ messages\ blocked?\ Or\ send\ reports?)\)
- Retracting a signal \((how\ do\ I\ undo?)\)
- What kind of signature \((e.g.,\ what\ happens\ if\ I\ change\ certs?)\)
Dispatch?

- LAMPS (though not S/MIME specific)?
- Other options?