Memory Hole: Cryptographic protection for e-mail headers

Daniel Kahn Gillmor <dkg@aclu.org>

IETF 92

Dallas, March 2015

Leaky metadata in encrypted mail

```
From: Alice <alice@example.com>
To: Bob <bob@example.net>
Subject: Retirement plans
Date: Fri, 20 Mar 2015 08:11:06 -0500
Content-Type: multipart/encrypted;
   protocol="application/pgp-encrypted";  boundary=xxxxx

--xxxxx
Content-Type: application/pgp-encrypted

Version: 1

--xxxxx
Content-Type: application/octet-stream; charset=UTF-8

-----BEGIN PGP MESSAGE-----

WETYIXVbSZ4VWTBoxqJtQtszIfRmcJjq74QBRVXVjjbjZKH5uVrqn5EK
FiUeZ5V+5gkXqfYVziZWPAZDs6K6qV9kvDGs+v/ZZNS4aSf0Sx5FiGmf
...
```

Unsigned context for signed mail

```
From: Charles <charles@example.com>
To: Diane <diane@example.com>
Subject: The Jones Account
Content-Type: multipart/signed; micalg=pgp-sha256;
   protocol="application/pgp-signature"; boundary="xxxxx"

--xxxxx
Content-Type: text/plain; charset=us-ascii

It's a go.  Please bill them!

--xxxxx
Content-Type: application/pgp-signature;
name="signature.asc"

-----BEGIN PGP SIGNATURE-----

nWlpkpARYEyQswgLQkr/6/pMtyLhpMownAZBIZXLFc4upcKihpdZMmy
[...]
```

Not just `Subject:`

- `Message-Id:`
- `References:`, `In-Reply-To:`
- `User-Agent:`
- `From:`
- `To:`
- `Date:`
- `Cc:`
- …

Why is this an issue?

- Encryption:
  - Violates "end-to-end" goal of message encryption
  - Graph analysis on metadata is effective!
- Signing:
  - Header-replacement on signed messages is easy
- Difficult security property to explain

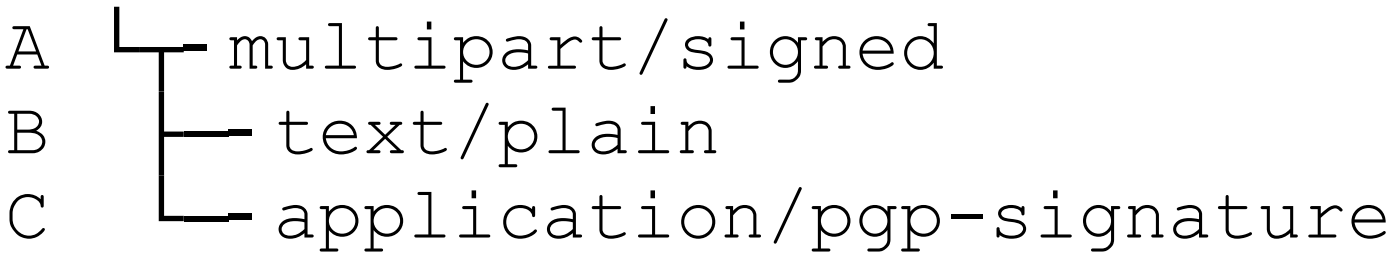
We can fix it

`Content-Type: text/rfc822-headers`

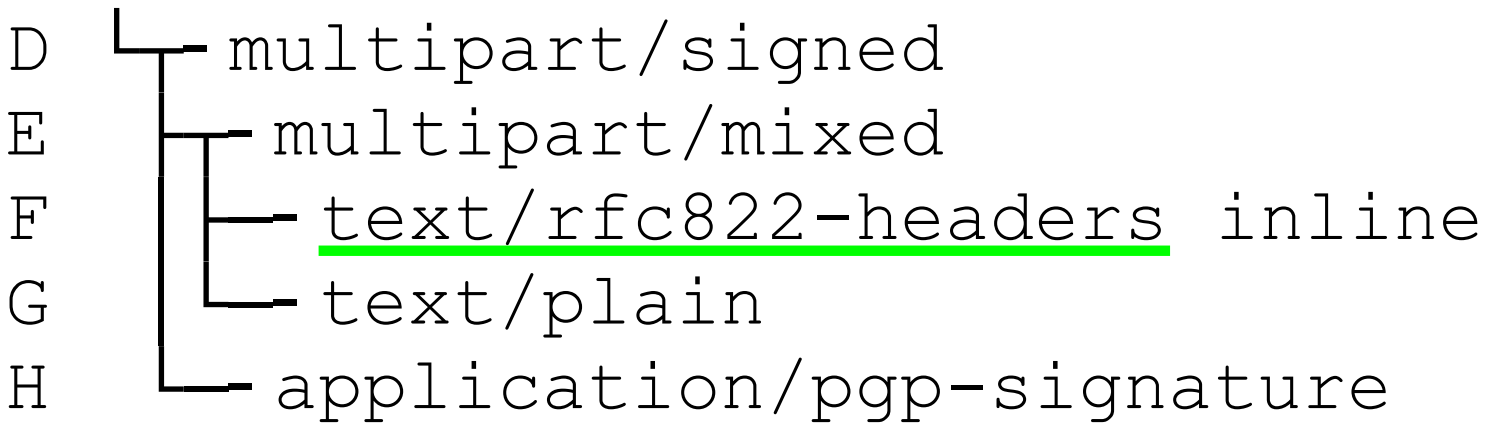
(RFC 6522 §4, currently only for DSN)

- Deployable now by improving sending MUAs
- Existing receiving MUAs OK
- Improves with updated receiving MUAs
- Improves more with compatible MTAs
- Designed with current spam abatement (DMARC, DKIM, SPF) in mind
- Currently OpenPGP-focused, some S/MIME demand

Signed Messages



becomes:



Encrypted Messages

```
A └─ multipart/encrypted
B   ├─ application/pgp-encrypted
C   └─ application/octet-stream
D        ↓
E        └─ text/plain
```

becomes:

```
F └─ multipart/encrypted
G   ├─ application/pgp-encrypted
H   └─ application/octet-stream
I        ↓
J        └─ multipart/mixed
K          ├─ text/rfc822-headers inline [correct header]
L          └─ text/plain
```

With dummy header on outside!

Phased deployment

- Sending, Encrypting MUAs
- Sending, Signing MUAs
- Receiving MUAs
- MTAs

Signalling

- Per-message?
  - Don't need? Detect by presence of `text/rfc822-header` part in the right place
- Per-recipient?
  - How do we know recipient prefers memory-hole messages? Should we just send them anyway?

Followup

- Discussion currently happening on:
  - <openpgp@ietf.org>
  - moved there from <gnupg-devel@gnu.org>