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

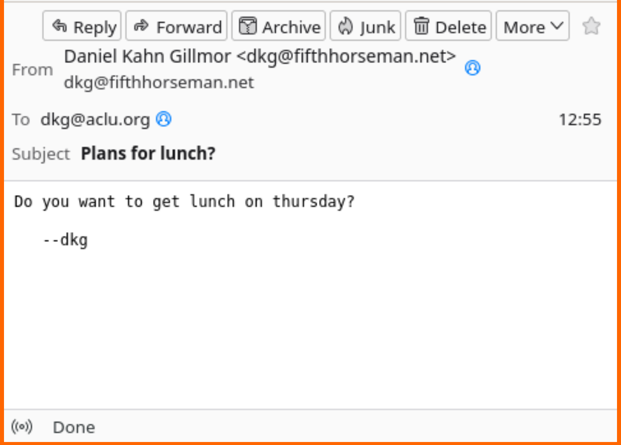
Why don’t people send signed mail?

- 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?



From Daniel Kahn Gillmor <dkg@fifthhorseman.net>
dkg@fifthhorseman.net

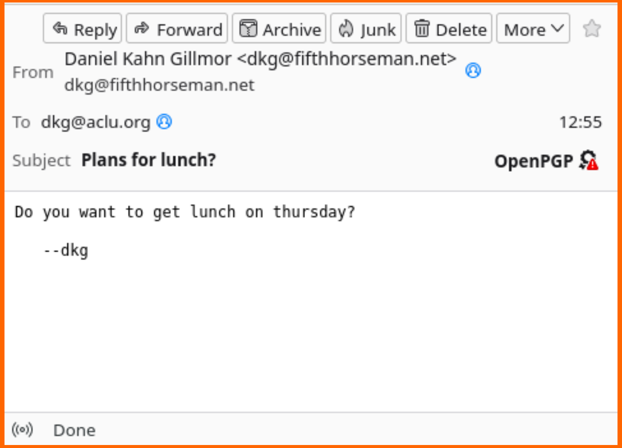
To dkg@aclu.org 12:55

Subject **Plans for lunch?**

```
Do you want to get lunch on thursday?

    --dkg
```

Unannotated



From Daniel Kahn Gillmor <dkg@fifthhorseman.net>
dkg@fifthhorseman.net

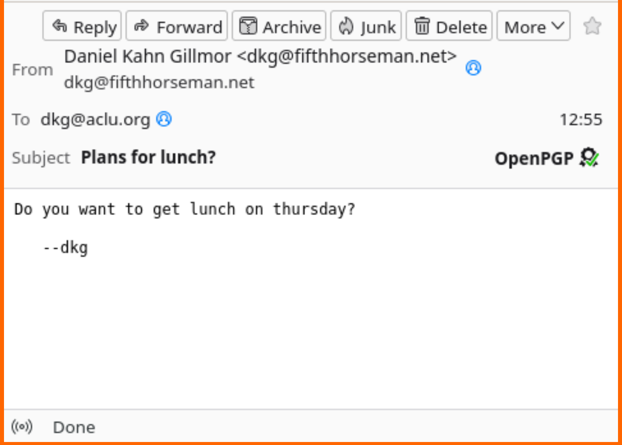
To dkg@aclu.org 12:55

Subject **Plans for lunch?** **OpenPGP**

```
Do you want to get lunch on thursday?

    --dkg
```

Broken



From Daniel Kahn Gillmor <dkg@fifthhorseman.net>
dkg@fifthhorseman.net

To dkg@aclu.org 12:55

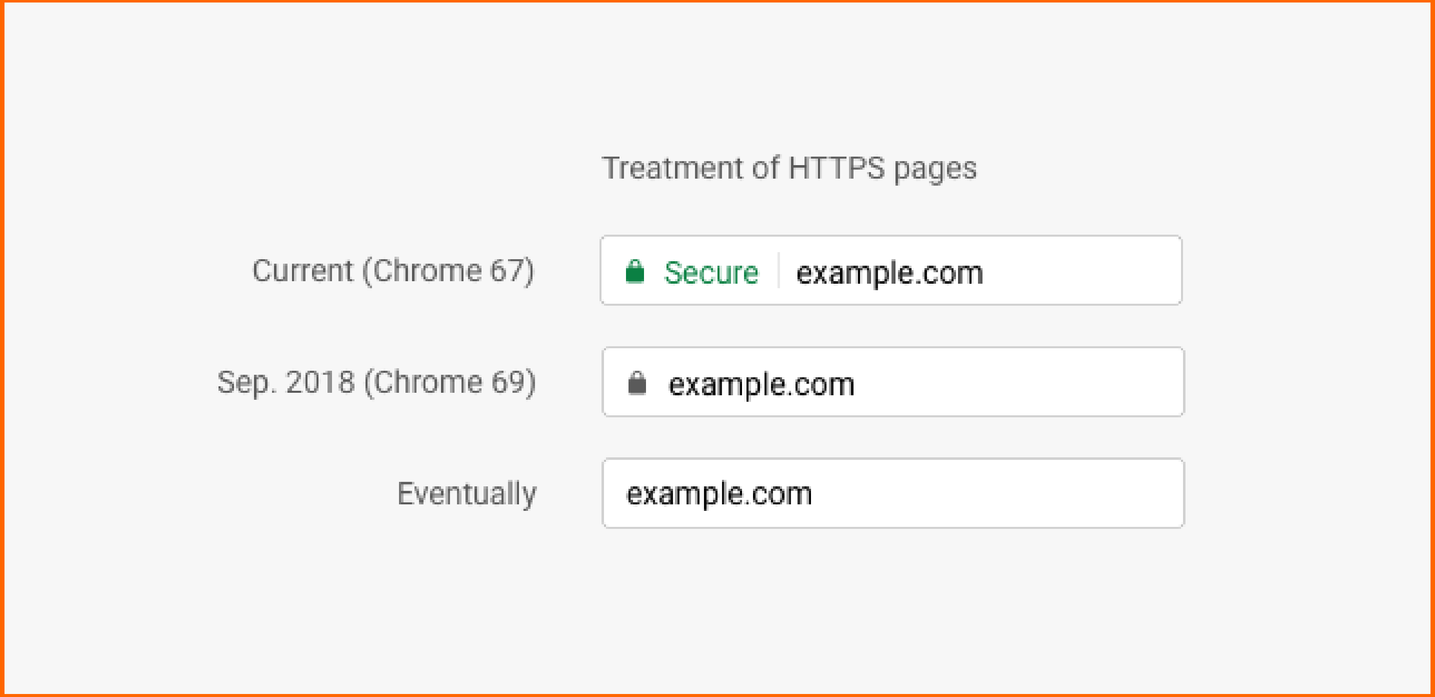
Subject **Plans for lunch?** **OpenPGP** ✓

```
Do you want to get lunch on thursday?

    --dkg
```

Signed

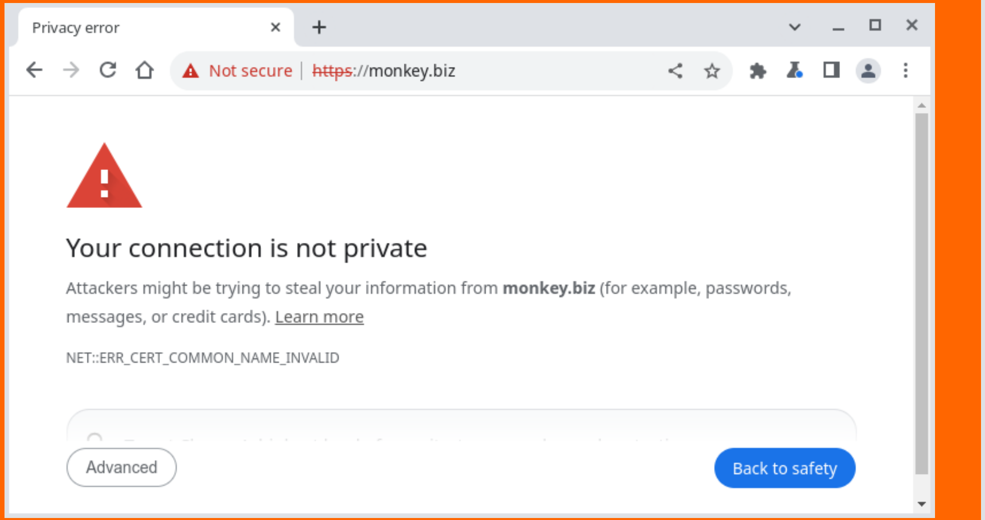
Where have we seen this before?



Treatment of HTTPS pages

Current (Chrome 67)	🔒 Secure | example.com
Sep. 2018 (Chrome 69)	🔒 example.com
Eventually	example.com

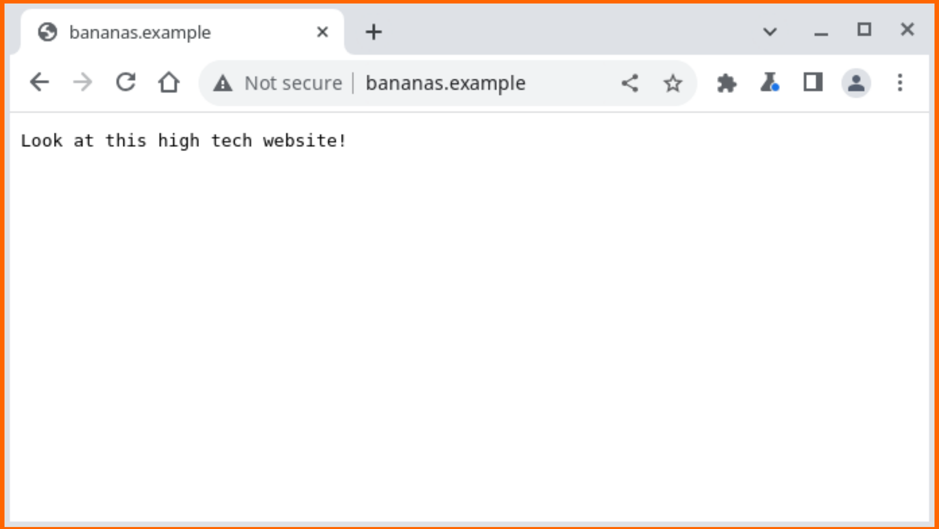
Continuing the analogy to HTTPS...



Your connection is not private

Attackers might be trying to steal your information from **monkey.biz** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID



```
Look at this high tech website!
```

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 signatues
- draft-ietf-lamps-e2e-mail-guidance “Future Work” §A.8 “expectations of cryptographic protections”

Decisions

- Signal location (*e-mail header? Depends on* `draft-ietf-lamps-header-protection`)
- Signal scope (*all messages* ***`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?