Encrypted E-mail for Planet Earth: Failures, Challenges, and the Future

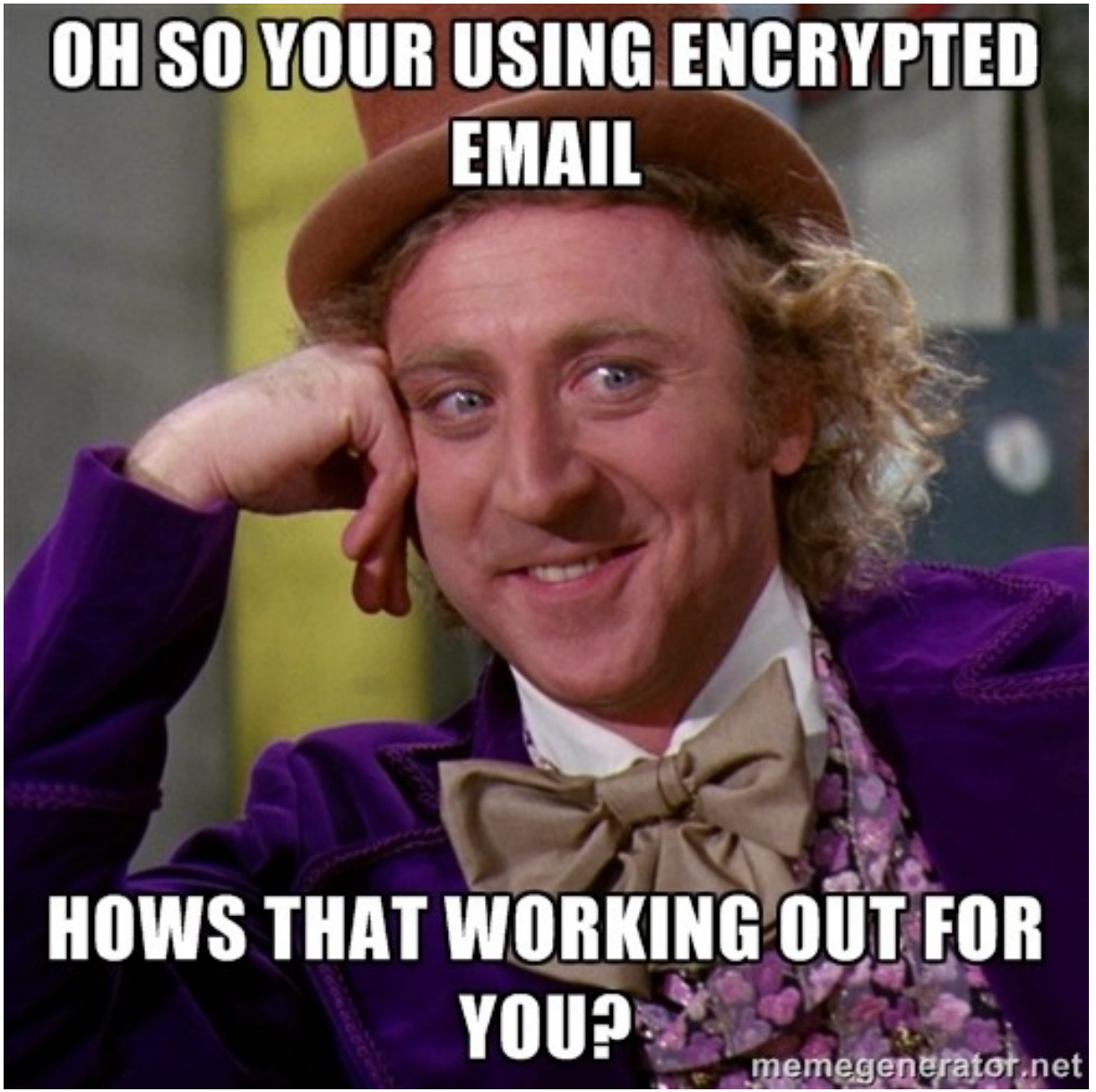
Harry Halpin (MIT)
@harryhalpin harry@w3.org

Meskio (LEAP)
meskio@sindominio.net

Gus Andrews (Simply Secure)
@gusandrews

Evan Henshaw-Plath (Crafted)
@rabble

Why aren't all messages encrypted?



GREAT PROJECTS EVERYWHERE

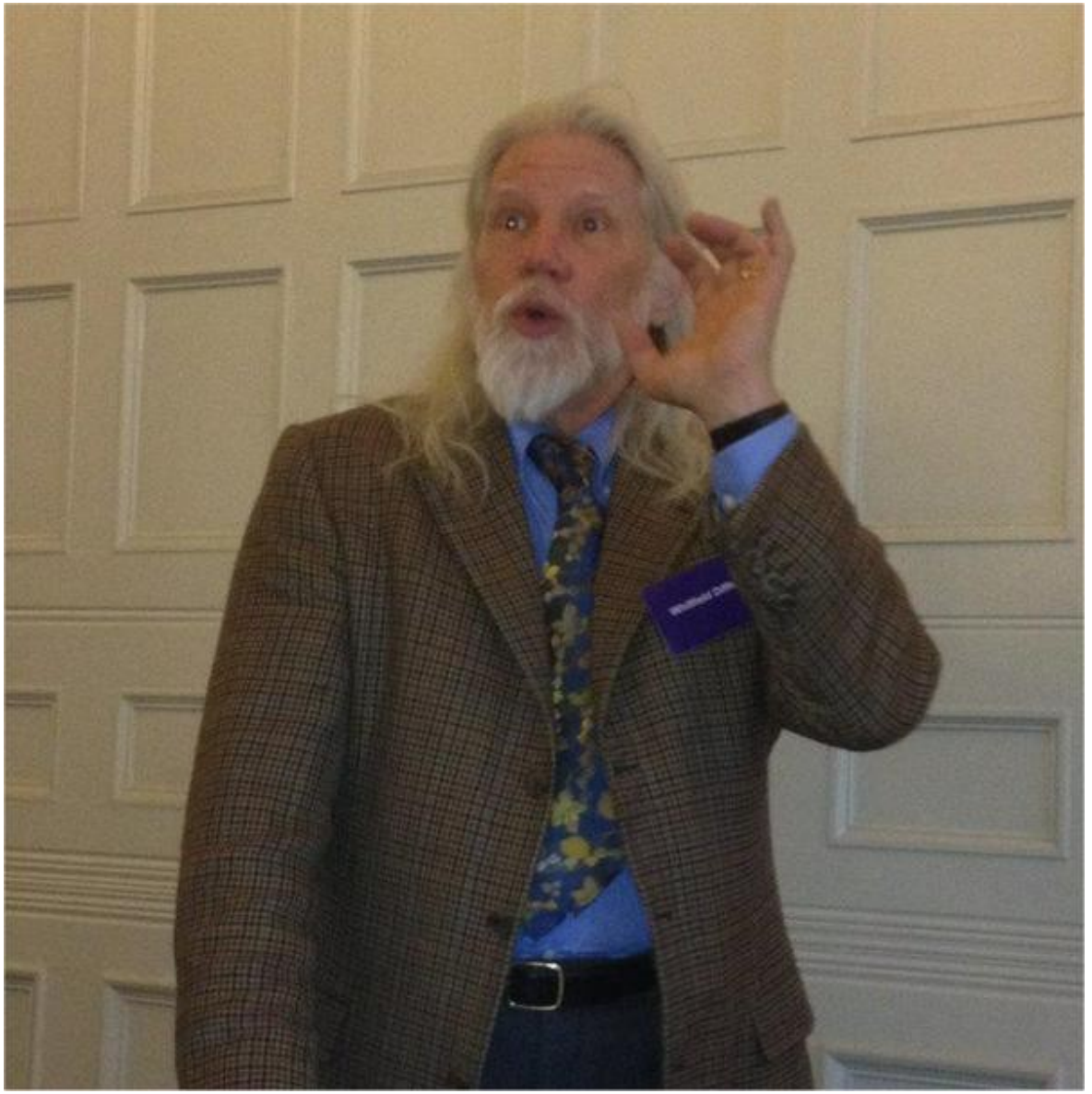
- **Enigmail: https://enigmail.net/**
- **GnuGPG: https://gnupg.org/**
- **Schleuder: http://schleuder2.nadir.org/**
- **LEAP Encryption Access Project: http://leap.se**
- **Mailpile: http://mailpile.se**
- **Pixelated: https://pixelated-project.org/**
- **Pond (Experiment!): https://pond.imperialviolet.org/**
- **Signal/TextSecure: https://whispersystems.org/**

Why isn't the Net encrypted by default?

- **TCP/IP (Kahn and Cerf): 1973**
- **Public-Key Crypto (Diffie-Hellman) 1976:**
- **RSA: 1977**
- **SMTP (Postel): 1982**
- **OpenPGP (Zimmerman): 1991**

“ I worked with the National Security Agency on the design of a secured version of the internet but we used classified security technology at the time and I couldn't share that with my colleagues. If I could start over again I would have introduced a lot more strong authentication and cryptography into the system.”

Vint Cerf (Google Hangout)

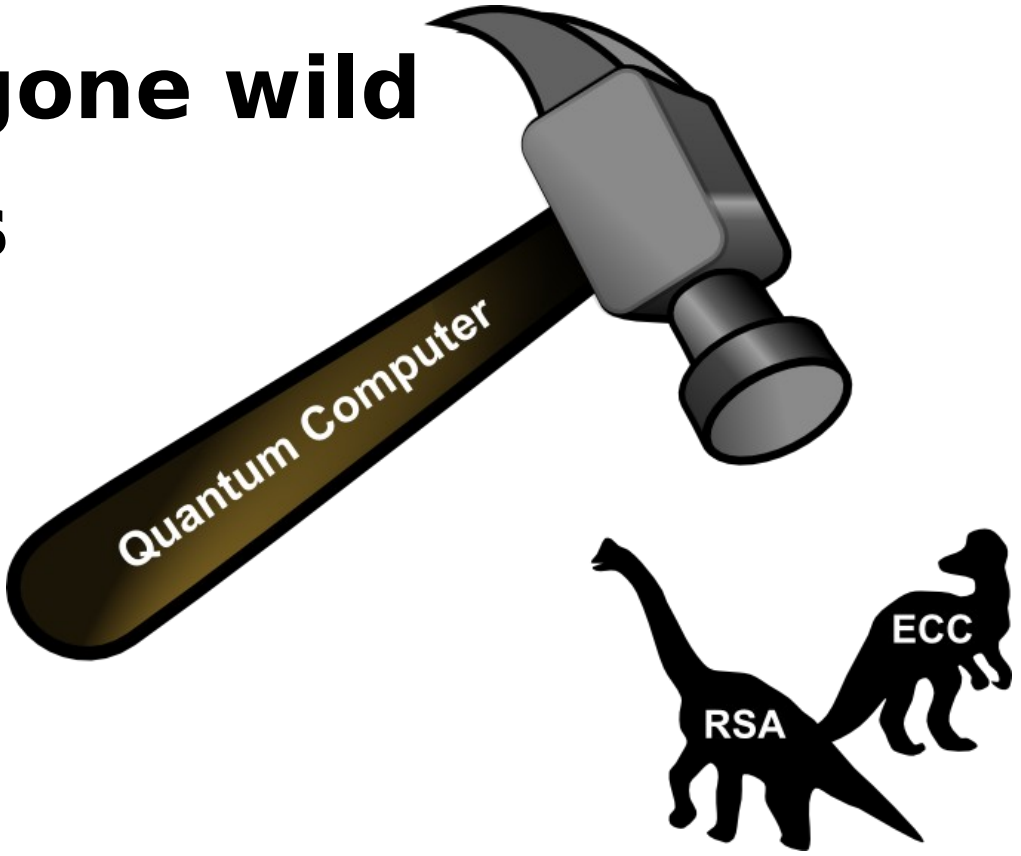


Bolting on Crypto

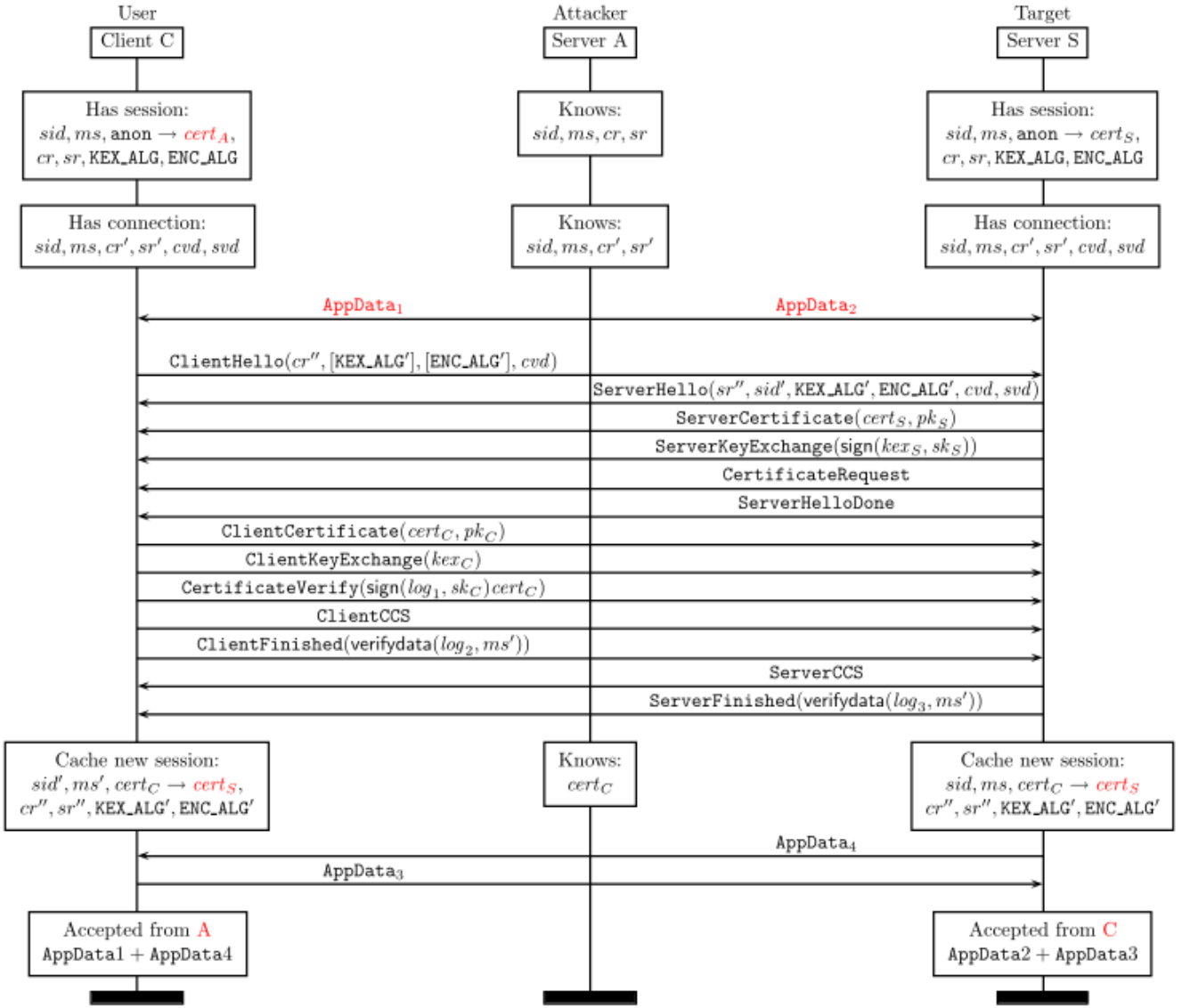
TCP/IP →IPSec (1995), Telnet → SSH (1995), FTP → SFTP (1997), HTTP→ TLS (SSL 1995), SMTP → OpenPGP (1991), Zimmerman, Bernstein...

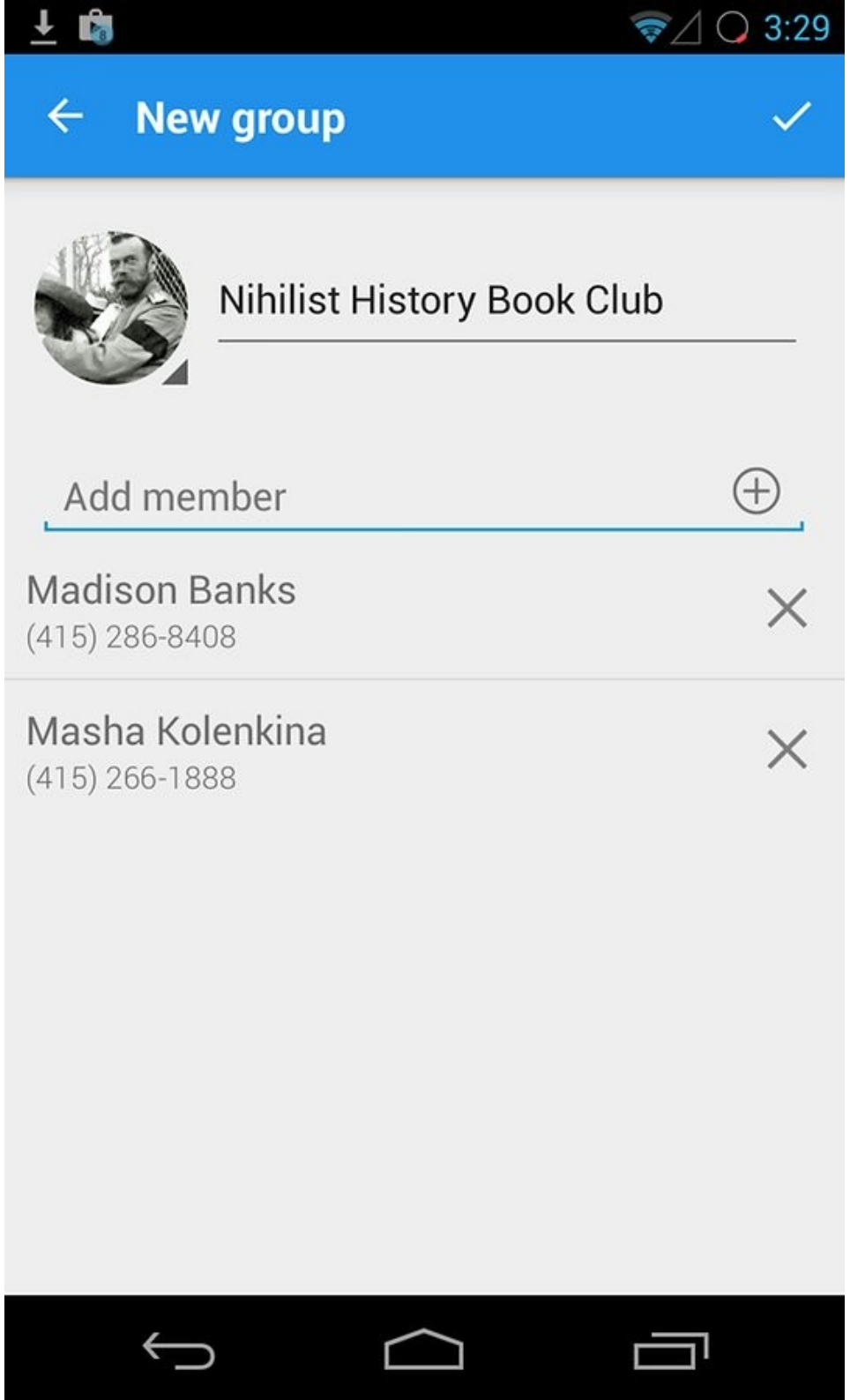
Designing Protocols is Hard

- **Computational Power Sky-rocketing**
- **Provable Security?**
- **Algorithm agility gone wild**
- **Legacy Algorithms**
- **New Algorithms**
- **Post-Quantum?**



VERY HARD


User
Client C
Attacker
Server A
Target
Server S
Has session:
$sid, ms,$ anon $\rightarrow cert_A$,
$cr, sr,$ KEX_ALG, ENC_ALG
Knows:
sid, ms, cr, sr
Has session:
$sid, ms,$ anon $\rightarrow cert_S$,
$cr, sr,$ KEX_ALG, ENC_ALG
Has connection:
$sid, ms, cr', sr', cvd, svd$
Knows:
sid, ms, cr', sr'
Has connection:
$sid, ms, cr', sr', cvd, svd$
AppData$_1$
AppData$_2$
ClientHello(cr'', [KEX_ALG'], [ENC_ALG'], cvd)
ServerHello(sr'', sid', KEX_ALG', ENC_ALG', cvd, svd)
ServerCertificate($cert_S, pk_S$)
ServerKeyExchange(sign(kex_S, sk_S))
CertificateRequest
ServerHelloDone
ClientCertificate($cert_C, pk_C$)
ClientKeyExchange(kex_C)
CertificateVerify(sign(log_1, sk_C)$cert_C$)
ClientCCS
ClientFinished(verifydata(log_2, ms'))
ServerCCS
ServerFinished(verifydata(log_3, ms'))
Cache new session:
$sid', ms', cert_C \rightarrow cert_S$,
cr'', sr'', KEX_ALG', ENC_ALG'
Knows:
$cert_C$
Cache new session:
$sid, ms, cert_C \rightarrow cert_S$
cr'', sr'', KEX_ALG', ENC_ALG'
AppData$_4$
AppData$_3$
Accepted from A
AppData1 + AppData4
Accepted from C
AppData2 + AppData3



Designing Privacy-Preserving Protocols is EVEN HARDER

Post E-mail and Decentralization

(mp)OTR:
http://www.cypherpunks.ca/~iang/pubs/mpotr.pdf

SCIMP (Silent Circle):
https://silentcircle.com/products-and-solutions/technology/scimp/

Axlotl (OpenWhisper):

https://github.com/trevp/axolotl/wiki

OpenWhisper Group Messaging:
https://whispersystems.org/blog/private-groups/

THE NET NEEDS YOU

Modern Crypto: https://moderncrypto.org/

IETF OpenPGP WG: https://datatracker.ietf.org/wg/openpgp/documents/

W3C Security IG http://www.w3.org/Security/wiki/IG

Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications: http://dspace.mit.edu/handle/1721.1/97690

Almost 25 years of PGP

and “no one” uses it

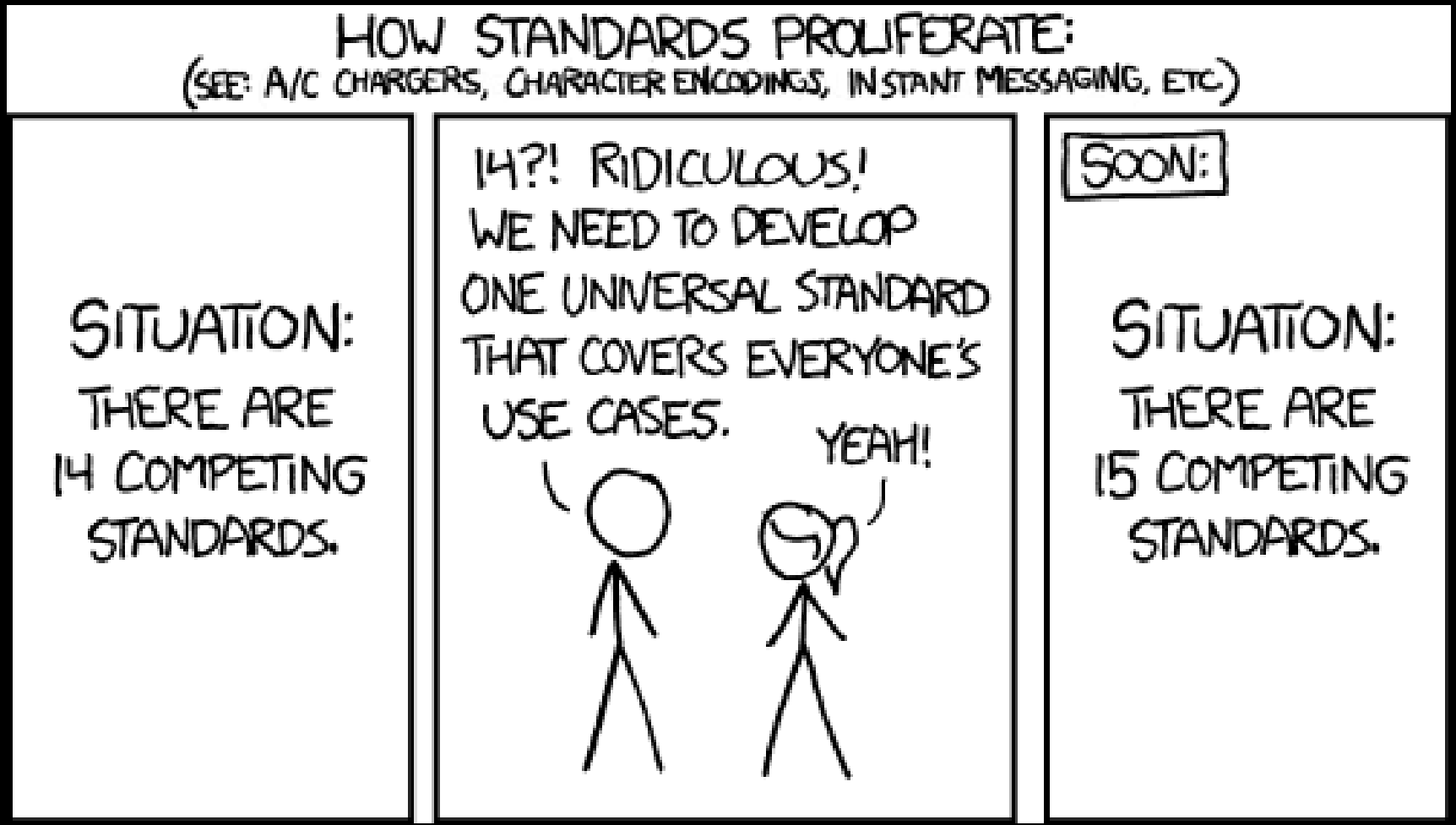
OpenPGP problems

- Metadata leakage
  - Web of Trust
  - Heathers/smtp
- Forward secrecy
- Key management
- Learning curve
- ...

Are they actually OpenPGP problems?

Or email and implementation problems?

Replace email?



Can we fix email?

(or improve it?)

Hard problems

- Key management
- Availability
- Asynchronous
- Meta-data
- Group communication
- ...

Memory hole

Email C:

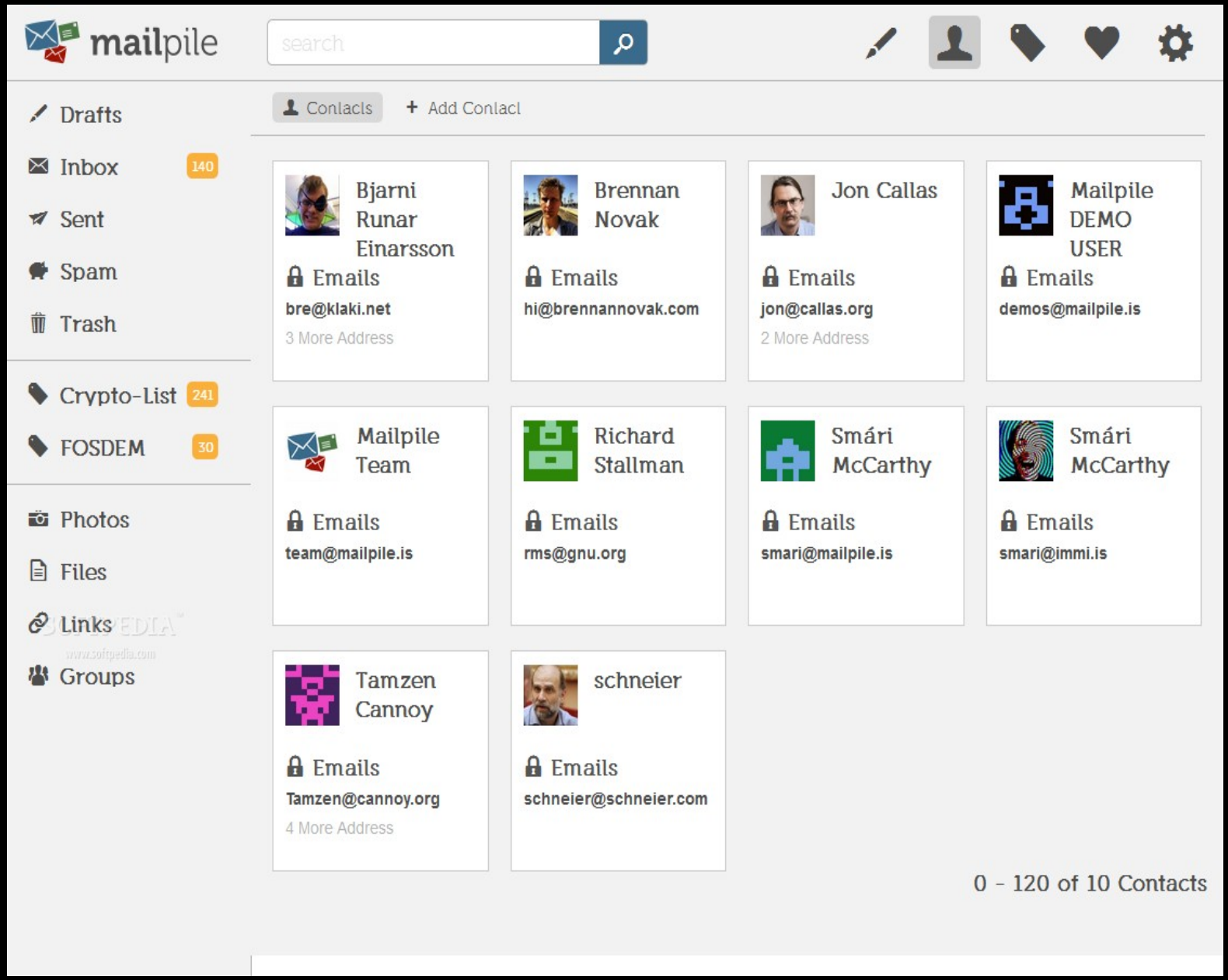
alternative text/html message with embedded header, signed, with Subject tampered

```
└─┬ multipart/signed 1706 bytes (Subject: the subject has been tampered!)
  ├─┬ multipart/mixed 850 bytes
  │ ├── text/rfc822-headers attachment 228 bytes
  │ └─┬ multipart/alternative 450 bytes
  │   ├── text/plain 86 bytes
  │   └── text/html 202 bytes
  └── application/pgp-signature 455 bytes
```

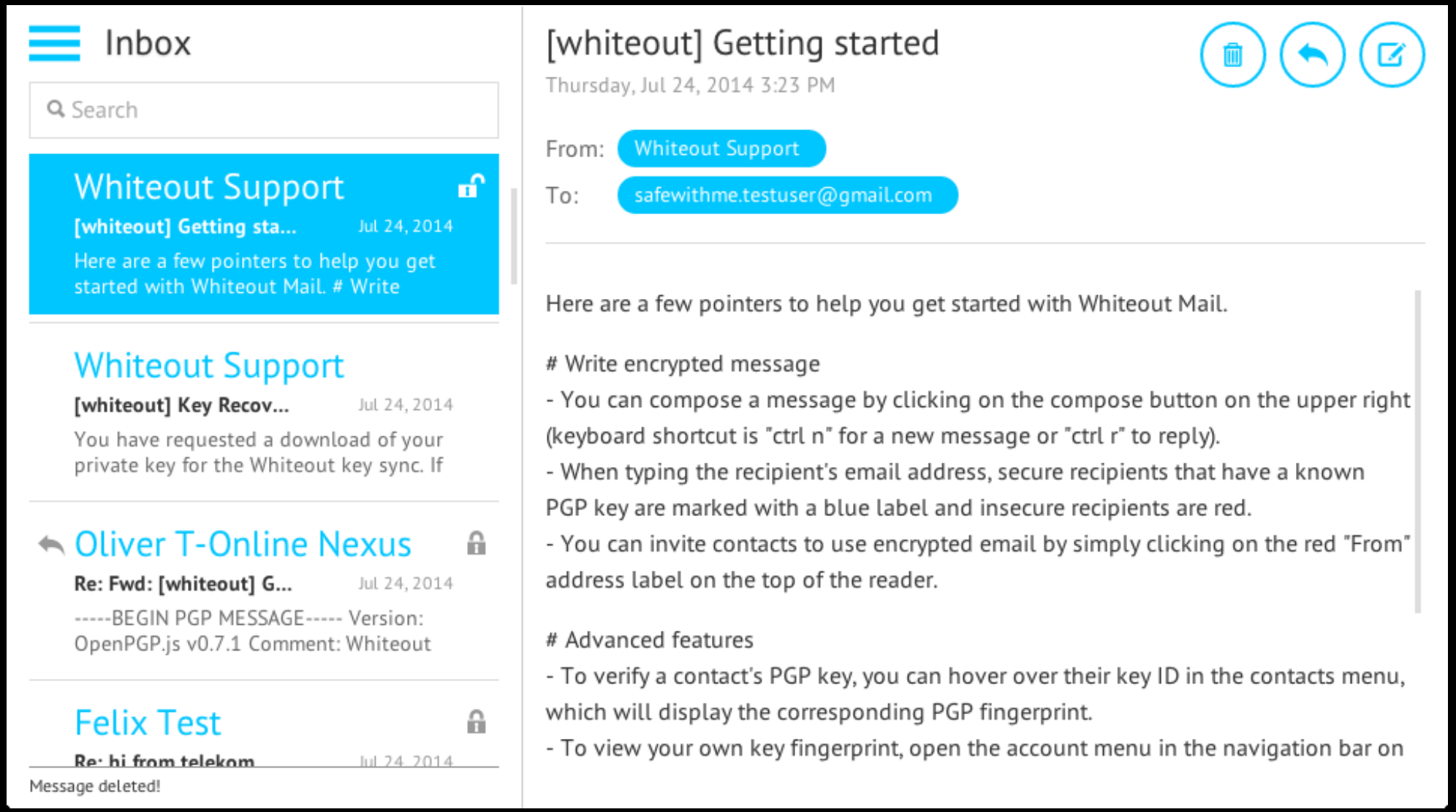
http://modernpgp.org/memoryhole/

http://www.coniks.org/

https://leap.se/



https://mailpile.is/



https://whiteout.io/