



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

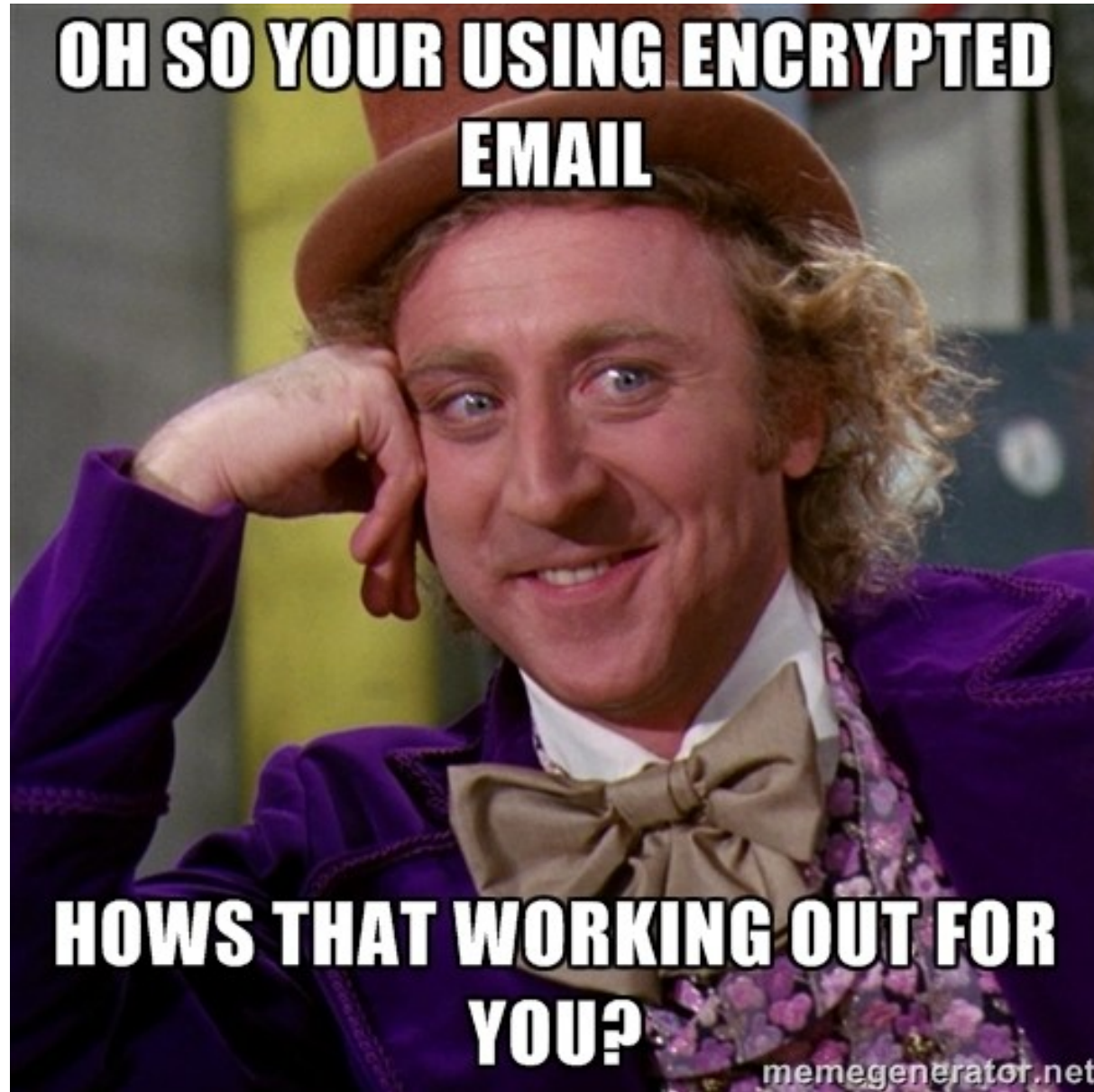
Harry Halpin (MIT)
@harryhalpin harry@w3.org

Meskio (LEAP)
meskio@sindominio.net

Gus Andrews (Simply Secure)
@gusandrews

Evan Henshaw-Plath (Crafted)
@rabble

Why aren't all messages encrypted?



GREAT PROJECTS EVERYWHERE

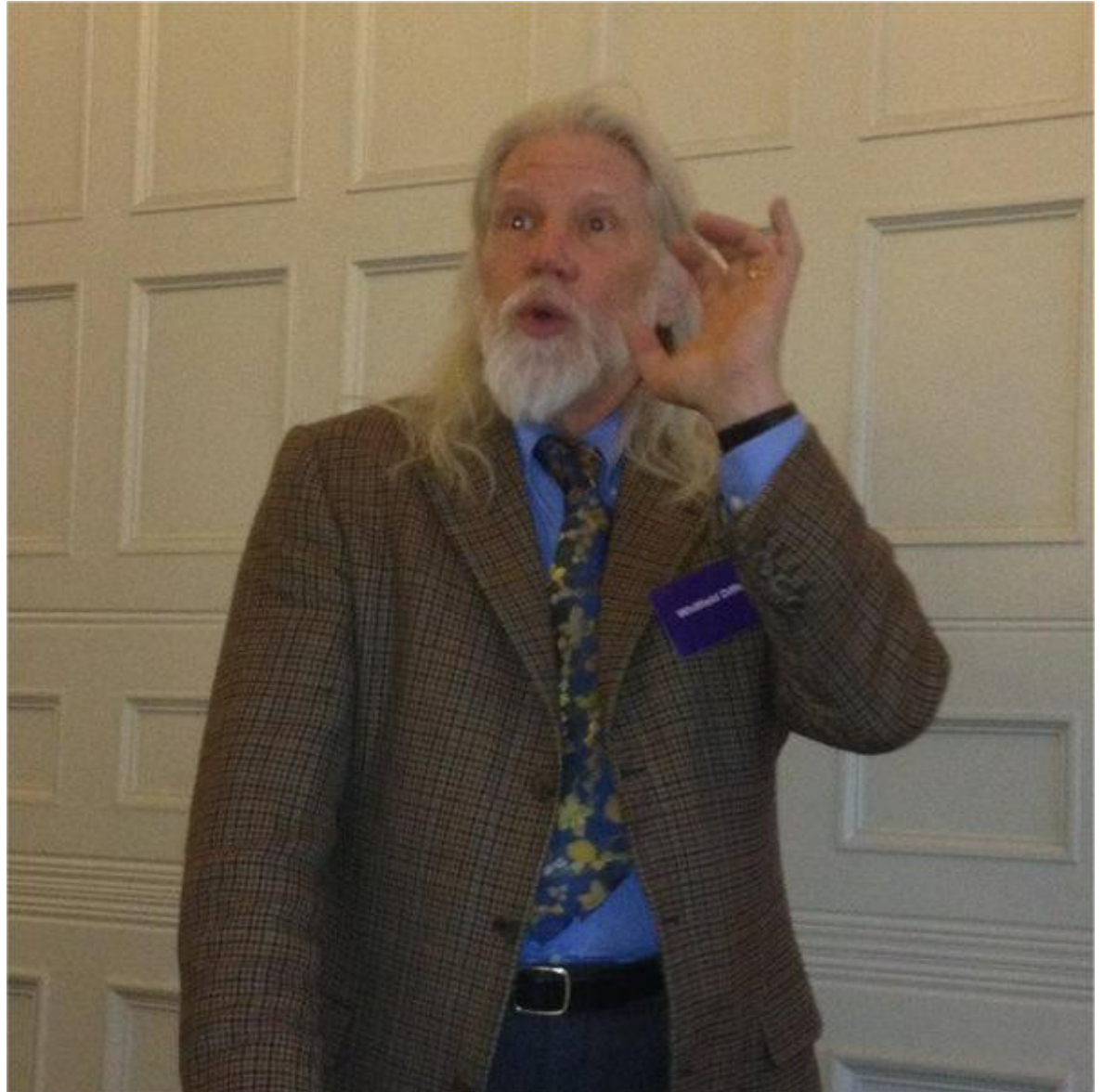
- Enigmail: <https://enigmail.net/>
- GnuPG: <https://gnupg.org/>
- Schleuder: <http://schleuder2.nadir.org/>
- LEAP Encryption Access Project: <http://leap.se>
- Mailpile: <http://mailpile.se>
- Pixelated: <https://pixelated-project.org/>
- Pond (Experiment!):
<https://pond.imperialviolet.org/>
- Signal/TextSecure: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



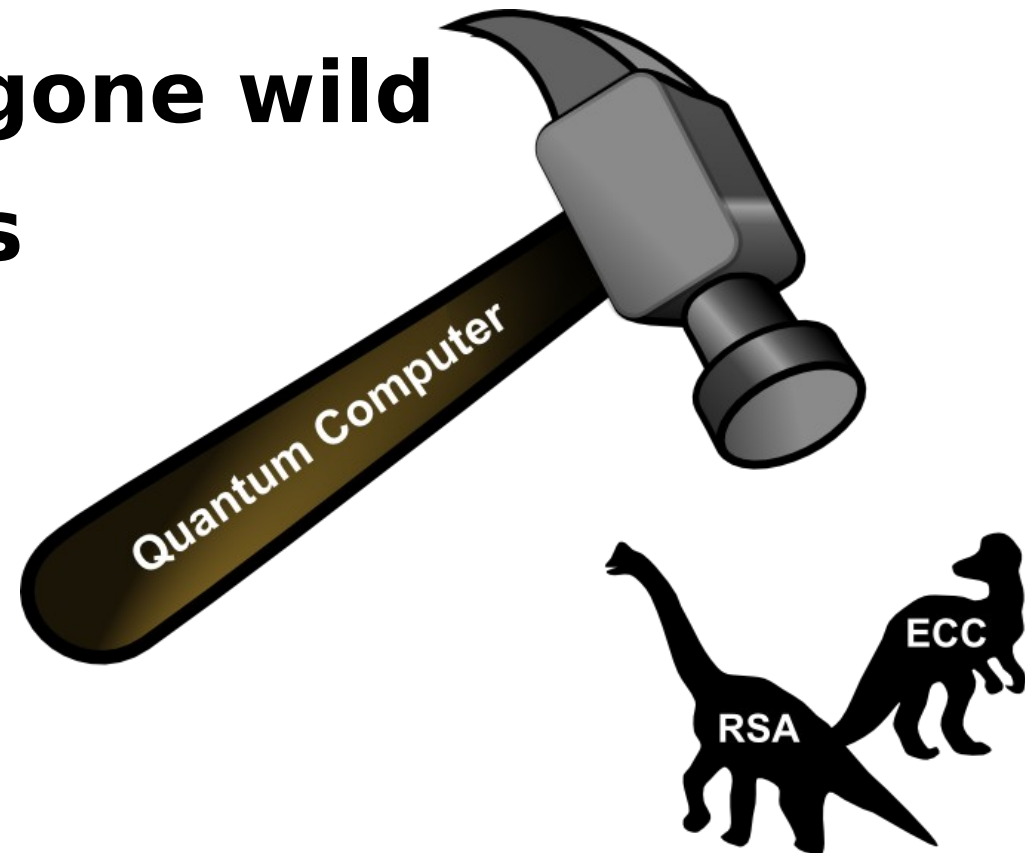
Bolting on Crypto

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

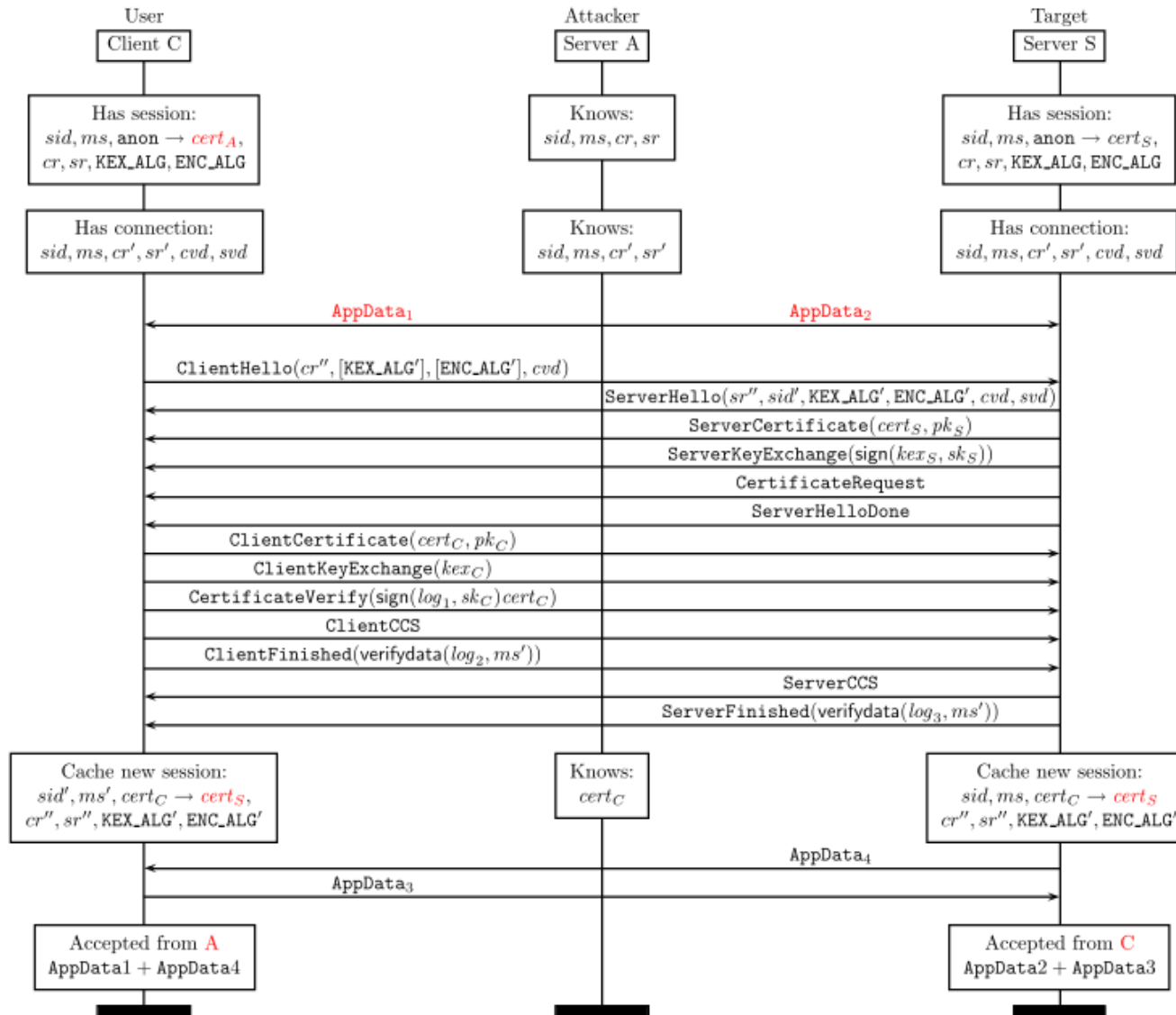


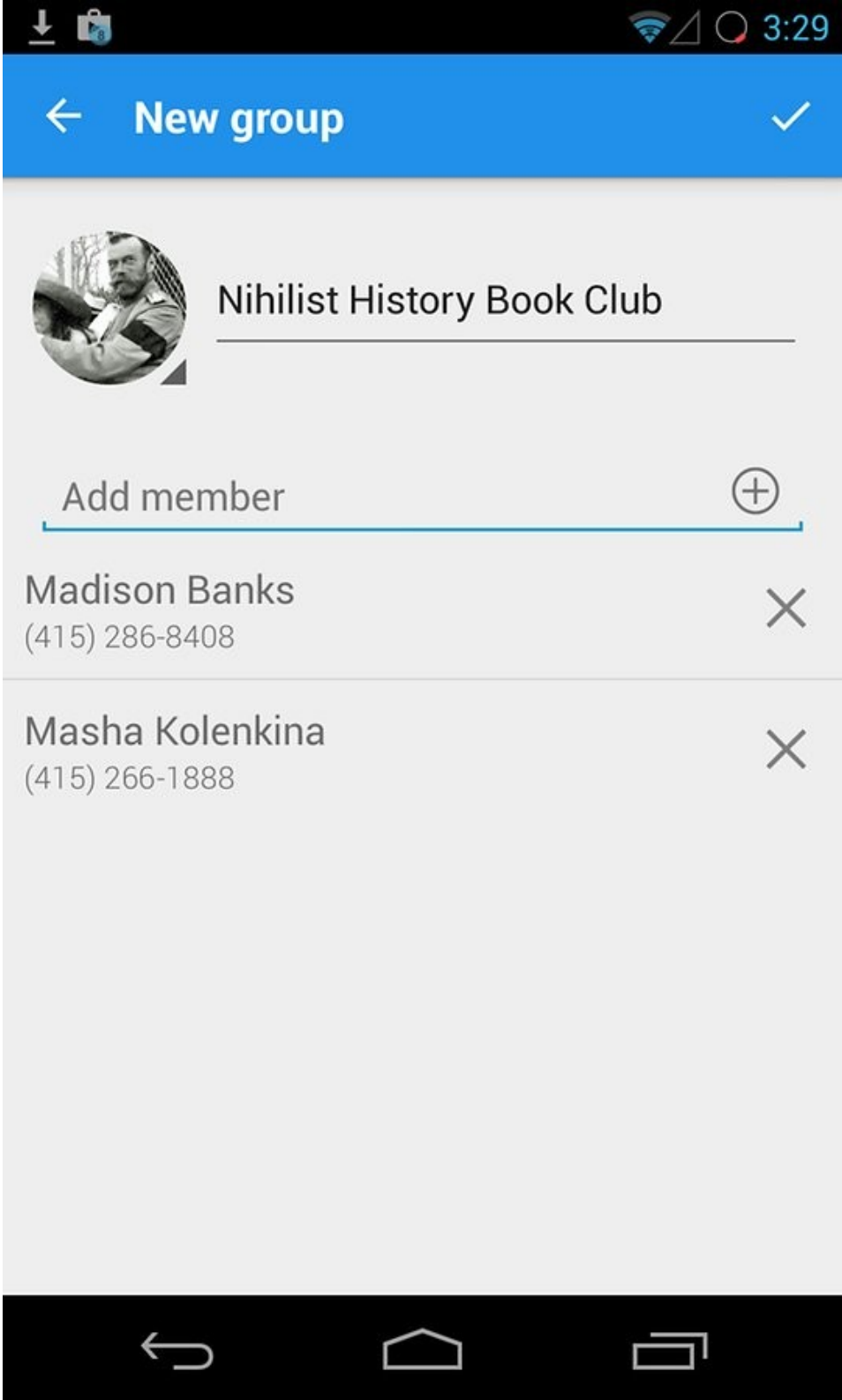
Designing Protocols is Hard

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



VERY HARD





**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?

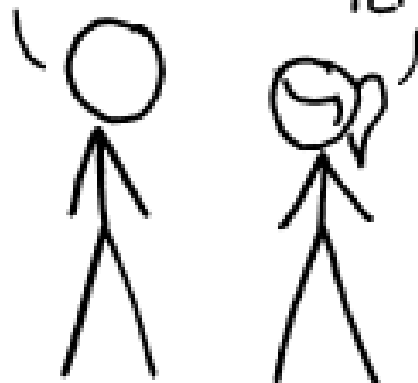
Or email and implementation
problems?

Replace email?

HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)

SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.



SOON:

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

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/>

CONIKS

Preserving Secure Communication through
Practical Key Verification for End Users.

<http://www.coniks.org/>



<https://leap.se/>



Drafts

Inbox

140

Sent

Spam

Trash

Crypto-List

241

FOSDEM

30

Photos

Files

Links EDIA

www.softpedia.com

Groups

Contacts

+ Add Contact



Bjarni Runar Einarsson

🔒 Emails
bre@klaki.net
3 More Address



Brennan Novak

🔒 Emails
hi@brennannovak.com



Jon Callas

🔒 Emails
jon@callas.org
2 More Address



Mailpile DEMO USER

🔒 Emails
demos@mailpile.is



Mailpile Team

🔒 Emails
team@mailpile.is



Richard Stallman

🔒 Emails
rms@gnu.org



Smári McCarthy

🔒 Emails
smari@mailpile.is



Smári McCarthy

🔒 Emails
smari@immi.is



Tamzen Cannoy

🔒 Emails
Tamzen@cannoy.org
4 More Address



schneier

🔒 Emails
schneier@schneier.com

0 - 120 of 10 Contacts

<https://mailpile.is/>

Inbox

Search

Whiteout Support

[whiteout] Getting sta... Jul 24, 2014

Here are a few pointers to help you get started with Whiteout Mail. # Write

Whiteout Support

[whiteout] Key Recov... Jul 24, 2014

You have requested a download of your private key for the Whiteout key sync. If

Oliver T-Online Nexus

Re: Fwd: [whiteout] G... Jul 24, 2014

-----BEGIN PGP MESSAGE----- Version: OpenPGP.js v0.7.1 Comment: Whiteout

Felix Test

Re: hi from telekom Jul 24, 2014

Message deleted!

[whiteout] Getting started

Thursday, Jul 24, 2014 3:23 PM

From: Whiteout Support

To: safewithme.testuser@gmail.com

Here are a few pointers to help you get started with Whiteout Mail.

Write encrypted message

- You can compose a message by clicking on the compose button on the upper right (keyboard shortcut is "ctrl n" for a new message or "ctrl r" to reply).
- When typing the recipient's email address, secure recipients that have a known PGP key are marked with a blue label and insecure recipients are red.
- You can invite contacts to use encrypted email by simply clicking on the red "From" address label on the top of the reader.

Advanced features

- To verify a contact's PGP key, you can hover over their key ID in the contacts menu, which will display the corresponding PGP fingerprint.
- To view your own key fingerprint, open the account menu in the navigation bar on

<https://whiteout.io/>