SMIMP, Email, Superglue

A discussion on the state of email security, and options for a path forward.

Email security today...

The Email Failfest

- Assumes network is trusted
- Assumes servers are trusted
- Assumes the sender is who they claim
- Doesn't prevent content modification
- Doesn't protect content

Torch it, or keep trying to fix it?

Keep:

- Massive user base
- Deeply entrenched
- Universal support

Torch:

- Do it right
- Strong crypto
- Better privacy

SMIMP: A Micro Introduction

- End-to-end Crypto (curve25519)
- Forward secrecy (loosely based on TextSecure)
- Integrated public key discovery
- Hash-chain to detect profile alteration
- Dynamic Hashcash-like proof of work
- Transported over HTTPS (firewall friendly, harder to block or inspect)

The Two Sides of SMIMP

Identity

- Name
- Public Ed25519 key
- Web site
- Social profiles

Messaging

- Multiple message types
- Whitelist / blacklist / anti-spam
- Simple JSON format

What's the status today?

- Spec work still ongoing
- No code written
- Needs more feedback

Thanks!

smimp.org
github.com/smimp/smimp_spec

adam@adamcaudill.com
@adamcaudill