MATHMESH BOF

Phillip Hallam-Baker

10am Monday Collyer
Make computers easy to use by making them more secure

• Cryptographically connect every device Alice owns to each other
  • Alice’s personal Mesh
  • Use that framework to authenticate maintenance messages
  • Enable use of strong end-to-end encryption

• 3 Core problems
  • Provision private keys to devices
  • Provide the means to obtain and validate public keys
  • Secure data at rest
Security today

- SSH
- OpenPGP, S/MIME
- Signal, Keybase, WhatsApp, etc. etc.
- Anti-virus
- NAT / VPN
- Spam filtering

- Separate products, separate dashboards
  - Security falls between the cracks
Mesh Core

- UDF: Naming, ‘Cryptography on Rails’
- DARE: Cryptographic envelopes, sequences
- Meta-Cryptography: Key splitting/combination

- IoT
- OpenPGP
- S/MIME
- 2nd Factor
- SSH
- Contact
Why choose passwords?

Sorry but your password must contain an uppercase letter, a number, a haiku, a gang sign, a hieroglyph, and the blood of a virgin.
MATHMESH BOF

10am Monday Collyer

Videos, Documents: http://mathmesh.com/