The Mathematical Mesh

Phillip Hallam-Baker

Venture Cryptography

Internet security is broken

- Users find security too much effort
  - Can’t solve that by sending users on a two day course
- Applications don’t solve the real security problems
  - Data at Rest
- We haven’t changed our approach
  - Using 1980s techniques to solve 21st century problems

Three core problems

- Device management
- Contact management
- Secure control messaging
  - End-to-end secure
  - Traffic analysis resistance friendly (32KB)

Radical distrust

- Can’t trust device manufacturers
- Can’t trust service providers

- Have to trust someone
  - Separation of duties
    - Can’t trust any single provider
    - Put limited trust in multiple provider

Meta-Cryptography

- 1 Key cryptography was good
- 2 was better
- Using 3 or more keys allows separation of duties
  - The cloud service can control who can decrypt, but can’t decrypt

Small, powerful concepts

- UDF Fingerprints describe direct trust relations
- Mesh Profiles describe trust axioms
  - Encoded as a DARE Envelope
- Catalogs, Spools are DARE Containers
  - Append only sequences of DARE envelopes
- Mesh accounts manage collections of catalogs and spools

The project: Meetup Monday 18:10

- Speak now, it will be hard to change things after deployment
- 8 Internet drafts
- MIT License reference code (C#)
  - SciKit Learn for cryptography
  - An easy way to secure applications
  - Can use features individually or as a package
    - Functionality of blockchain, PKCS#7, PGP, X.509, etc. etc.
    - One coherent platform, same encoding and approach throughout.