The Mathematical Mesh

Phillip Hallam-Baker

Venture Cryptography
Internet security is broken

• We haven’t changed our approach
  • Using 1980s techniques to solve 21st century problems

• 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
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
The Mesh is a platform

• What do we need to support Muti-party decryption?
  • Managing private keys across a user’s (proliferating) devices
  • Acquiring and maintaining the public keys of other users (and services)
  • Secure control plane messaging

• Each component is designed for re-use
  • Engineered as if a stand-alone features
  • Reducing the size of the Mesh code
  • Increasing applicability

• Deployment strategy identifies applications with unilateral benefit
Principal technology platforms

• UDF
  • Naming & Addressing

• DARE Envelope & Container
  • Message layer security ‘PCKS#7 with blockchain on steroids using JOSE)
  • Persistence model, catalogs and spools

• Mesh Assertions
  • Describe users, devices, accounts, services and connections between

• Mesh Messaging
  • Control plane messaging. End to end secure, traffic analysis resistant
UDF Uniform Data Fingerprint

• Represent any cryptographic output as a Base32 sequence
  • Content Digest
    • MB5S-R4AJ-3FBT-7NHO-T26Z-2E6Y-WFH4 (SHA-2)
    • KCM5-7VB6-IJXJ-WKHX-NZQF-OKGZ-EWVN (SHA-3)
  • Nonce
    • ND2H-S6YN-5PEI-7VCC-EABR-WQLC-QVTQ
  • Encryption key master secret
    • EBYX-SP24-RAEZ-BYVG-FJEN-TNW6-EYQQ
  • Shamir Secret Share
    • SAQH-5KQR-XCVN-UVWY-OJNB-QTG3-MJSM-I
  • HMAC result
    • ADUE-MT5J-2IED-MT4Y-5C2B-7FK7-UJQW
Express as a URI

• udf://example.com/EBE4-KH3S-2YBP-LVBR-Y5SW-LGH4-IR2G-HG

• UDF (EBE4-KH3S-2YBP-LVBR-Y5SW-LGH4-IR2G-HG) =
  • MB4X-FCXI-V5LX-LKMP-7O6T-DEOS-NWSJ-DXJN-QOGM-WOFZ-INCN-QBAY-QBLC-XA5K

Encode as a QR code

Alice May Brock
Restauranteur
Great Barrington, Massachusetts
DARE Envelope / Container

- Envelope
  - PKCS #7 in JOSE / JSON-B
  - Support multiple key decryption (Alice+Service)

- Container
  - Append only sequence of DARE Envelopes
  - Blockchain/Merkle-Tree type capabilities
  - Incremental Encryption
    - Apply one key exchange to multiple envelopes
Applications

• Mesh Account
  • Catalog (set of items)
    • Passwords / Contacts / Bookmarks / Applications
  • Spools (list of messages)

• Log format for GDPR compliance
• ZIP Archive replacement
Radical Distrust

- Mesh Accounts belong to the user
  - They can be bound to a service ID
  - The user can change that at any time
  - Low switching cost

- Use alice@example.com to discover a trust relationship
  - Use UDF digest to persist it
Mesh Messaging

• Secure Control plane
  • End-to-end secure
  • Anti-Abuse measures built in
  • Traffic Analysis Resistant
    • Messages padded/truncated at 32KB in transport

• Applications
  • Secure contact exchange
  • Two Factor Authentication (OTP Code)
  • Confirmation Service (Semantic binding to action)
Where do we go from here?

• IETF / W3C / OASIS / New?

• If IETF
  • Is this actually IRTF?
  • Start a working group? More than one?
  • Experimental?

• Will begin deploying this year
  • End-to-end secure password manager
  • SSH / OpenPGP / S/MIME configurator