Towards a Threshold Key Infrastructure

Phillip Hallam-Baker
Threshold Secrets
What is a Threshold Key Infrastructure?

- **Public Key Infrastructure** manages the Public keys
  - What is Alice’s encryption Key?
  - Is this really Alice’s signature key?

- **TKI** manages the Private keys
  - Smartcards: The Achilles’ heel of PKI deployment
    - Every device Alice owns has a set credentialed private keys
  - Device keys are established using Threshold Generation
  - Use of account keys is gated by threshold techniques
    - The lost device problem
    - The insider threat problem (Snowden, Manning)
Why is this relevant?

- TKI makes PKI easy to use
  - Zero User Impact usability
    - Save/Load documents from Word, Excel, PowerPoint: No user experience changes
    - Send/Receive email: No user experience changes
    - End to End secure discussion board: No user experience changes
- TKI demonstrates value of certain threshold techniques
  - In most cases \([ n, t ] = \{ 2, 2 \} \text{ or } \{ 3, 2 \} \text{ or } (\text{possibly}) \{ 5, 3 \}\)
  - Currently using simplest constructions
  - Enterprise deployment MAY require more sophisticated approaches
- TKI gives user control
  - Zero Trust or Better Than Zero Trust can be achieved
Example: Mesh Password Vault

• Mesh service (alice@example.com) provides synchronization
  • Password vault is encrypted under \{a.P, a\}
  • Service cannot decrypt

• Alice has 6 devices connected to her Mesh
  • For each device \(i\)
    • Create a new key split \(d_i + c_i = a\)
    • Device receives \(d_i\)
    • Service receives \(c_i\)
  • If Alice loses a device
    • Tells service no to respond to decryption requests.
    • BTZT: We do trust the service after all (just not so very much)
The Mathematical Mesh  [https://mathmesh.com/](https://mathmesh.com/)

- Replay the CERN Web Deployment strategy

- Open Specification + Services + Reference code (Dec 2020)
  - Windows, OSX and Linux (C# dotnet Core)
  - Student Project Friendly
    - Undergraduate
      - End to end encrypted social media / chat / etc.
      - User centered IoT
    - Postgraduate
      - Separation of duties in enterprise environments
      - Proofs / Protocol improvements

- Commercial products (2022 on)
  - TBA