WHY DID WE MAKE SECURITY SO HARD?

Phillip Hallam-Baker
Vice President and Principal Scientist
Comodo Group Inc.
Advanced?

People aren’t using basic yet
The Mathematical Mesh

- Open Specification
- MIT License Reference code
- Contemporary approach
  - JSON / Ed448/Curve448 / Web Service / etc.
  - Untrusted cloud service (end-to-end security)

- http://mathmesh.com/
Bad security is worse than no security
The best security is the security you use
Usability labs tell you how users behave in usability labs
Ask nothing of the user
Any instructions you can write for the user can be turned into code and executed by the machine.
Automate Certificate issue and rollover
Personal PKI

- Cost: Long term signature key
- Each user requires
  - Long term master signing key
  - Short term application profiles
What if?
Key Escrow

- Cost: Master Escrow Key

- Each user requires
  - Long term master signing key
  - Long term master escrow key
  - Short term application profiles
Offline Master Root

- Cost: Intermediate PKI layer

- Each user requires
  - Master Profile
    - Long term master signing key
    - Long term master escrow key
  - Current Profile
    - Administrative signing key
  - Short term application profiles
Offline Master Root

- **Cost:** Profile per device

- **Each user requires**
  - Master Profile
    - Long term master signing key
    - Long term master escrow key
  - Current Profile
    - Administrative signing key
  - Short term application profiles
  - Device profiles
Connection Protocol

apache@mathmesh.com
Hypothesis

- It is possible to solve any security usability issue by introducing an additional layer of PKI
Application profiles

Current applications
- SSH
- S/MIME
- OpenPGP
- XMPP (planned)

New applications
- Mesh/Recrypt
  - Data at rest encryption (DARE)
- Mesh/Catalog
  - Contacts/Credentials/2\textsuperscript{nd} factor
- Mesh/Unify
Killer Application?
How scripts leak credentials

#!/bin/bash
Username="Fred"
Password="ItsGonnaLeak"
Why did we make security so hard?
Apply

- Demand Effortless Security
- Choices:
  - Consider Mathematical Mesh as a Proof of Concept
  - Mesh-Enable your applications