Der Weg zur einfachen Verschlüsselung

Werner Koch

GUUG FFG — München, 2. März 2012

Outline

Why we Need End-to-End Encryption

Bei der Übermittlung sensibler Inhalte —- etwa von Gesundheitsdaten —- müssen nun die verantwortlichen Stellen, etwa die Krankenkassen, für eine Ende-zu-Ende-Verschlüsselung sorgen.

(Peter Schaar)

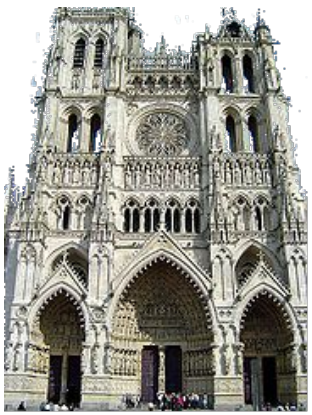
Why Mail Encryption is a Total Failure

Failed Approaches

For over 15 years we tried:

- New features
- Banning of export restrictions
- Getting rid of patents
- Telling spy tales
- Legislative requirements
- Improving user interfaces
- Building crypto appliances
- Using centralized crypto

What's wrong with PKIs?



As a result there's no pressure on the people involved in PKI standardisation to create anything that meets any real-world requirement, allowing them instead to spend their time building great gothic cathedrals of infinite complexity whose sole purpose seems to be to strike awe and terror into the masses.
– Peter Gutmann

Automatic Key Generation

- Bind key to the mail address
- Default key parameters
- Generate a key in the background
- Create self-signed certificates for S/MIME

What About the Passphrase

- Personal information management service (PIM service) is required anyway:
  - Appointments, phone numbers, address book, bookmarks, desktop configuration, mail accounts, other profile data.
  - For mobility.
  - All this data is sensitive.
- The private key is just another item to store in a PIM service
- Unify key passphrases and PIM service access
- Temporary solution is needed for now.

Automatic Key Distribution

- Keyservers don't scale
- X.509 LDAP is even worse
- No way to delete a key
- Solution: DNS
  - Decentralized and highly available
  - Mail addresses in the DNS are easy
  - Easy to manage DB
  - DNSSEC improves initial key validity

Opportunistic Encryption

- 25% accidentally sent mail in the clear
- We want security by default
- Filters/agents are too complicate to manage
- MUAs need to implement it directly
- All MUAs either provide S/MIME or PGP/MIME
- We choose a key which best matches the user's mainly used MUA.

TUFC/POP

- PKIX: Ask your parents first
- WoT: Do what your peers suggest
- Our model should better map user's expectations.

- The SSH model is build on this:
  - TUFC = Trust Upon First Contact
  - POP = Persistence Of Pseudonyms
- Revocations are done by removing the key from the DNS.

Infrastructure

- The user must be able to manage the DNS record
- Automation protocol for key generation and storage
  (e.g. Extending IMAP)
- Key rollover and revocation mechanism
  (phone hot line, SMS based confirmation)

Key Generation

- Automatic key generation if no key is setup for an account
- For X.509 use a dummy CA instead of directly self-signed certificates
- All done in the background
- Notifications by mail
- Integration with PIM service

Changes to GnuPG

- Use GnuPG as the backend
  - Available for all platforms
  - S/MIME and OpenPGP
  - Matured software
- Has almost all required features
- Need to add a local database with observed mail/key associations
- Add API to create a key in the background
- Key backup/restore using QRcodes

MUA Changes

- Automatically create a key
- Tell GnuPG about the sender address
- Configure option to disable the TUFC/POP model
- Extend the backup feature (PIM service?)

Expert Options

- Allow using one key for several accounts
- The PKA protocol uses an indirection and thus allows for it.
- Option to disable TUFC/POP
- Option to weight TUFC/POP and conventional trust schemes

User Interface

- We need high quality feedback
- A few UI elements are still required
- Optional notification that a mail will be sent in the clear
- Initiate a key revocation or rollover
- Restore a backup
- How to show a conflict (key change)

Mail Providers

- We need their support!
- It needs to be tightly integrated
- Implementation of automation protocols
- Key revocation confirmation

Web-mailers

- That is browser based crypto
- Implement using extension modules
- PIM service is important
- A fallback solution would be based on Javascript

Searching

- Searching through encrypted mails is time consuming
- Searching via IMAP even harder
  (you don't want to decrypt the mails on the server)
- Adding a separate symmetric storage key may speed up things.
- Use an encrypted index database
  (Prototype implementation for Kontact)

Spam

- Out of scope!
- Someone else needs to work on it.
- Content filtering needs to be done at the client.

What if the Titanic Sinks

In case public key crypto meets the iceberg we will have the infrastructure to quickly setup a system based purely on symmetric keys.

Future Work

- Find a mail provider for a prototype implementation
- Design protocols for automation
- Write an I-D for PKA
- Implement the contact database
- Change MUAs

More Info

http://g10code.com/steed.html