MEDUP

Missing Elements for Decentralized Usable Privacy

PEARG @ IETF-106, Mon Nov 18, 2019

Bernie Hoeneisen
<bernie.hoeneisen@pep.foundation>

Privacy by Default.
Background

- Decentralized (E2E / P2P)
  - Pervasive monitoring (RFC 7258) is an attack on Privacy
  - Centralized elements are more prone to attacks

- Usable
  - Message encryption is a hassle for most Internet users
    - Even for savvy users, setting up encryption may take several hours
  - Need to fix this usability challenge by automation

- Privacy
  - Privacy is a Human Right (RFC 8280)
MEDUP in short

- Enhancements to application protocols for decentralized usable privacy
  - Based on Opportunistic Security (RFC 7435) principles
- Originally emerged from pEp (pretty Easy privacy)
  - Everybody working in this field (e.g. autocrypt) invited to participate & actively contribute to MEDUP
- Goal
  - Define the missing pieces (e.g. key management, private key synchronization, message formats, trustwords, handshake, etc.)
MEDUP Group

- Non-WG sessions during IETF meetings
- Mailing list discussion:
  - medup@ietf.org
  - To subscribe: https://www.ietf.org/mailman/listinfo/MEDUP
- Aims for BoF/ IETF WG
I-D Dependency Graph

Legend:
- Core: Secure decentralized synchronization
- Handshake & trust: pEp Applications
- pEp Applications

Requirements
- Threat Analysis

Trustwords (IANA Registry)
- pEp Trust rating & UI Mapping (trust level → color/symbol/text)

pEp core (pgp/enc/auth)
- pEp Handshake
- pEp Key Reset

pEp Key sync
- pEp Key sync
- pEp email (incl. msg. formats)
- pEp Trust sync
  - other sync

pEp S/MIME
- other application

Handshake & trust
- pEp Applications

Legend:
- depends on
- uses / may use
- I-D exists
- Not pEp specific
- I-D coming soon
- TBD
Questions
Backup Slides
What MEDUP is about?

Missing Elements for Decentralized and Usable Privacy

The MEDUP list is for discussions of enhancements to application protocols for decentralized usable privacy.

RFC 8280 has identified and documented important principles in such as Data Minimization, End-to-End and Interoperability in order to enable access to Human Rights. While (partial) implementations of these concepts are already available, today's applications widely lack Privacy support that ordinary users can easily handle.

In MEDUP these issues are addressed based on Opportunistic Security (RFC 7435) principles. Updates/usage clarifications to application level protocols such as email and XMPP are in scope.

Privacy by Default.
Example Msg. flow (simplified)

User A
- Auto-Generate key pair (if no key yet)

Device A
- Privacy Status for B: Unencrypted
- A sends message to B (public key attached), not encrypted

Device B
- Auto-Generate key pair (if no key yet)

User B
- Privacy Status for A: Unencrypted

A sends message to B (public key attached), not encrypted

B sends message to A (public key attached), encrypted

User A and B compare their Trustwords over an alternative channel (e.g. phone line)

Privacy Status for B: Trusted
Privacy Status for A: Trusted

Write message
Read message
Display Trustwords
Confirm Trustwords

Write message
Read message
Display Trustwords
Confirm Trustwords

TOFU (Trust on first use)
pEp Email Format 2

Outer message (Subject: pEp)

Inner message: encrypted original email

Original headers & content

Public key

Privacy by Default.